Oracle® Identity Manager

Connector Guide for SAP User Management Engine

Release 9.1.0

E17554-01

May 2010

Oracle Identity Manager Connector Guide for SAP User Management Engine, Release 9.1.0

E17554-01

Primary Author: Lyju Vadassery

Contributing Authors: Devanshi Mohan, Alankrita Prakash

Contents

1 About the Connector

2 Deploying the Connector

3 Using the Connector

List of Figures

List of Tables

Preface

This guide describes the connector that is used to integrate Oracle Identity Manager Connector with SAP User Management Engine.

Audience

This guide is intended for resource administrators and target system integration teams.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at `http://www.oracle.com/accessibility/`.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/support/contact.html` or visit `http://www.oracle.com/accessibility/support.html` if you are hearing impaired.

Related Documents

For information about installing and using Oracle Identity Manager, see the Oracle Identity Manager documentation library.

For generic information about connectors, see *Oracle Identity Manager Connector Concepts*.

The following Oracle Technology Network page provides links to Oracle Identity Manager documentation:

`http://www.oracle.com/technology/documentation/oim1014.html`

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager Connectors documentation, visit Oracle Technology Network at

`http://www.oracle.com/technology/documentation/oim1014.html`

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1 About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with external, identity-aware applications. This guide discusses the connector that enables you to use SAP User Management Engine as a managed (target) resource of Oracle Identity Manager.

> **Note:** At some places in this guide, SAP User Management Engine has been referred to as the **target system**.

In the account management (target resource) mode of the connector, data about users created or modified directly on the target system can be reconciled into Oracle Identity Manager. This data is used to provision (allocate) new resources or update resources already assigned to OIM Users. In addition, you can use Oracle Identity Manager to provision or update SAP User Management Engine resources assigned to OIM Users. These provisioning operations performed on Oracle Identity Manager translate into the creation of or updates to target system accounts.

This chapter contains the following sections:

- Section 1.1, "Certified Components"
- Section 1.2, "Certified Languages"
- Section 1.3, "Connector Architecture"
- Section 1.4, "Features of the Connector"
- Section 1.5, "Lookup Definitions Used During Connector Operations"
- Section 1.6, "Connector Objects Used During Reconciliation"
- Section 1.7, "Connector Objects Used During Provisioning"
- Section 1.8, "Roadmap for Deploying and Using the Connector"

1.1 Certified Components

Table 1–1 lists certified components for the connector.

Table 1–1 Certified Components

Component	Requirement
Oracle Identity Manager	Oracle Identity Manager release 9.1.0.2 BP 04 or later See the following Oracle Technology Network Web page for information about certified components of Oracle Identity Manager: `http://www.oracle.com/technology/software/products/ias/files/idm_certification_101401.html`
JDK	JDK 1.5 or later
Target system	SAP User Management Engine running on SAP NetWeaver '04 SPS 14 or SAP NetWeaver 7.0 SPS 05
SAP GRC Compliant User Provisioning	You must configure the Compliant User Provisioning module included in SAP GRC versions 5.2 SP4 or later and 5.3 SP5 or later.
External code	The connector uses OpenSPML Toolkit 2.0 (openspml2-toolkit.jar). See Section 2.1.1.4, "Copying OpenSPML Toolkit 2.0" for more information about addressing this requirement.

1.2 Certified Languages

This release of the connector supports the English locale.

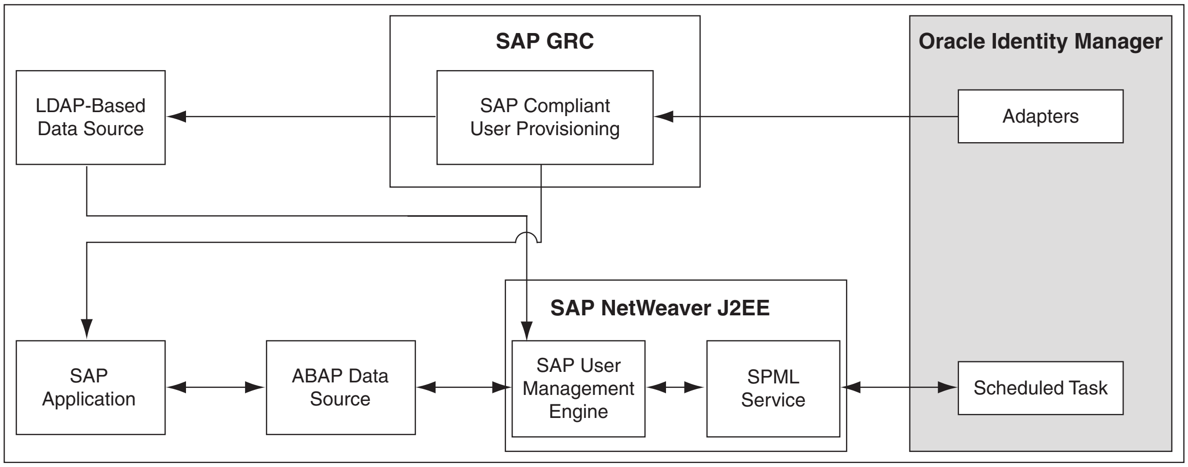
1.3 Connector Architecture

The connector sets up Oracle Identity Manager as the front end for sending account creation or modification requests to applications that use the data source linked with SAP User Management Engine. These requests are processed and then forwarded by the Complaint User Provisioning module of SAP GRC.

Account data added or modified through provisioning operations performed directly on the data source can be reconciled into Oracle Identity Manager through SAP User Management Engine.

Figure 1–1 shows the connector integrating SAP User Management Engine with Oracle Identity Manager.

Figure 1–1 Connector Integrating SAP User Management Engine with Oracle Identity Manager



As shown in the figure, SAP User Management Engine is configured as the management tool for user data stored on a data source, which is either the ABAP module or an LDAP-based solution. User data changes made through the SAP User Management Engine UI are reflected on the SAP applications that use the data source or on the UI of the LDAP-based solution.

By deploying the connector, you configure SAP User Management Engine as a target resource of Oracle Identity Manager.

Provisioning requests sent from Oracle Identity Manager are routed through SAP GRC to the application or system that uses the data source linked with SAP User Management Engine. User data changes resulting from the provisioning requests can be viewed through the SAP User Management Engine UI. Reconciliation is performed directly from SAP User Management Engine.

- Section 1.3.1, "Provisioning Process"
- Section 1.3.2, "Reconciliation Process"

1.3.1 Provisioning Process

During provisioning, adapters carry provisioning data submitted through the process form to the target system. The Compliant User Provisioning module of SAP GRC accepts provisioning data from the adapters, creates requests, and then forwards the requests to the application or system that forms the front end of the SAP User Management Engine data source.

In Compliant User Provisioning, workflows for processing these requests can be configured and users designated as approvers act upon these requests.

Reconciliation does not involve the Compliant User Provisioning module. Scheduled tasks on Oracle Identity Manager fetch data from the target system to Oracle Identity Manager.

The following is the detailed sequence of steps performed during a provisioning operation:

1. The provisioning operation is initiated through direct provisioning and access policy changes.
2. The connector sends requests and receives responses through the following Web services of SAP GRC:
   - SAPGRC_AC_IDM_SUBMITREQUEST: This Web service is used to submit requests.
   - SAPGRC_AC_IDM_REQUESTSTATUS: This Web service is used to fetch request statuses.
   - SAPGRC_AC_IDM_AUDITTRAIL: This Web service is used to check if there are error messages in the SAP GRC Compliant User Provisioning logs.

   The process form holds fields for both SAP User Management Engine and Compliant User Provisioning. However, for a Create User operation, only the Compliant User Provisioning fields (attributes) on the process form are used. Mappings for these fields are stored in the Lookup.SAP.CUP.ProvisionAttrMap and Lookup.SAP.CUP.ProvisionRoleAttrMap lookup definitions. If you specify values for any attribute that is not present in these lookup definitions, then the connector ignores those attributes during the Create User operation.

> **Note:** SAP GRC Compliant User Provisioning does not process passwords. During Create User provisioning operations, any value entered in the Password field is directly propagated to SAP User Management Engine.
>
> See Section 3.7, "Guidelines on Performing Provisioning" for information about setting passwords when you configure Compliant User Provisioning.

For a Modify User operation, a request is created only for attributes whose mappings are present in these lookup definitions. If you specify values for attributes that are not present in these lookup definitions, then the connector directly ignores those attributes.

3. When the request is created on SAP GRC Compliant User Provisioning, data sent back by Compliant User Provisioning is stored in the following read-only fields in Oracle Identity Manager:
   - Request ID: This field holds the request ID that is generated on SAP GRC Compliant User Provisioning. The request ID does not change during the lifetime of the request.
   - Request Status: This field holds the status of the request on SAP GRC Compliant User Provisioning. You configure and run the SAP CUP Status Update Recon scheduled task to fetch the latest status of the request from the target system. Section 3.5.3.3, "SAP CUP Status Update Recon" describes this scheduled task.
4. The request is passed through the workflow defined in SAP GRC Compliant User Provisioning. The outcome is one of the following:
   - If Compliant User Provisioning clears the request, then the outcome is the creation or modification of a user's account on the target system. The status of the request is set to Closed and a message is recorded in the Oracle Identity Manager logs.
   - If Compliant User Provisioning rejects the provisioning request, then the status of the request is set to Reject and a message is recorded in the Oracle Identity Manager logs.
   - If an error occurs during communication between Compliant User Provisioning and the target system, then the request remains in the Open state. A message stating that the operation has failed is recorded in the audit log associated with the request. An error message is displayed on the console.

1.3.2 Reconciliation Process

SAP NetWeaver AS Java offers an SPML 1.0 compliant interface to manage users, groups, and roles in SAP User Management Engine over a network. The scheduled task provided by the connector acts as the SPML client to send SPML requests to the SPML service in this application server.

During reconciliation, a scheduled task establishes a connection with the SPML service. Reconciliation criteria are sent through SPML requests to this SPML service. The SPML service processes the requests and returns SPML responses containing user records that match the reconciliation criteria. The scheduled task brings these records to Oracle Identity Manager.

Each record fetched from the target system is compared with SAP User Management Engine resources that are already provisioned to OIM Users. If a match is found, then the update made to the record is copied to the SAP User Management Engine resource in Oracle Identity Manager. If no match is found, then the user ID of the record is compared with the user ID of each OIM User. If a match is found, then data in the target system record is used to provision an SAP User Management Engine resource to the OIM User.

The process form holds attributes for both SAP User Management Engine and Compliant User Provisioning. However, only the SAP User Management Engine fields (attributes) on the process form are used for reconciliation. Mappings for these fields are stored in the Lookup.SAP.UME.ReconAttrMap and Lookup.SAP.UME.ReconChildAttrMap lookup definitions.

1.4 Features of the Connector

The following are features of the connector:

- Section 1.4.1, "Routing of Provisioning Requests Through SAP GRC Compliant User Provisioning"
- Section 1.4.2, "Full Reconciliation"
- Section 1.4.3, "Limited (Filtered) Reconciliation"
- Section 1.4.4, "Enabling and Disabling Accounts"
- Section 1.4.5, "Specifying Accounts to Be Excluded from Reconciliation and Provisioning Operations"
- Section 1.4.6, "Transformation and Validation of Account Data"

1.4.1 Routing of Provisioning Requests Through SAP GRC Compliant User Provisioning

Provisioning requests generated on Oracle Identity Manager are routed through SAP GRC Compliant User Provisioning. See Section 1.3.1, "Provisioning Process" for detailed information about this feature.

1.4.2 Full Reconciliation

> **Note:** The SPML UME API does not return records for which the Last Modified Date value is greater than a specified date. Therefore, the connector cannot support incremental reconciliation. This point is also mentioned in Section 5.2, "Connector Limitations Related to Features of the Target System."

In full reconciliation, all records are fetched from the target system to Oracle Identity Manager. The list of valid characters allowed in SAP is stored in the Lookup.SAP.UME.FullReconFilter lookup definition. During reconciliation, an SPML request is sent to the target system to fetch user IDs that start with these characters. The second SPML request is sent to fetch the details of these users.

During full reconciliation, a single reconciliation event is generated for each target system account.

1.4.3 Limited (Filtered) Reconciliation

To limit or filter the records that are fetched into Oracle Identity Manager during a reconciliation run, you can specify the subset of added or modified target system records that must be reconciled.

See Section 3.5.2, "Limited Reconciliation" for more information.

1.4.4 Enabling and Disabling Accounts

Valid From and Valid Through are two user attributes on the target system. For a particular user in SAP, if the Valid Through date is less than the current date, then the account is in the Disabled state. Otherwise, the account is in the Enabled state. The same behavior is duplicated in Oracle Identity Manager through reconciliation. In addition, you can set the value of the Valid Through date to a current date or a date in the past through a provisioning operation.

> **Note:** The Enabled or Disabled state of an account is not related to the Locked or Unlocked status of the account.

1.4.5 Specifying Accounts to Be Excluded from Reconciliation and Provisioning Operations

You can specify a list of accounts that must be excluded from all reconciliation and provisioning operations. Accounts whose user IDs you specify in the exclusion list are not affected by reconciliation and provisioning operations.

See Section 2.3.5, "Setting Up the Lookup.SAP.UME.ExclusionList Lookup Definition" for more information.

1.4.6 Transformation and Validation of Account Data

You can configure validation of account data that is brought into or sent from Oracle Identity Manager during reconciliation and provisioning. In addition, you can configure transformation of account data that is brought into Oracle Identity Manager during reconciliation. The following sections provide more information:

- Section 4.1, "Configuring Validation of Data During Reconciliation and Provisioning"
- Section 4.2, "Configuring Transformation of Data During User Reconciliation"

1.5 Lookup Definitions Used During Connector Operations

Lookup definitions used during connector operations can be categorized as follows:

- Section 1.5.1, "Lookup Definitions Synchronized with the Target System"
- Section 1.5.2, "Preconfigured Lookup Definitions"

1.5.1 Lookup Definitions Synchronized with the Target System

During a provisioning operation, you use a lookup field on the process form to specify a single value from a set of values. For example, you use the Role lookup field to select a role from the list of roles defined on the target system. When you deploy the connector, lookup definitions corresponding to the lookup fields on the target system are automatically created in Oracle Identity Manager. Lookup field synchronization involves copying additions or changes made to the target system lookup fields into the lookup definitions in Oracle Identity Manager.

> **Note:** The target system allows you to use special characters in lookup fields. However, in Oracle Identity Manager, special characters are not supported in lookup definitions.

The Lookup.SAP.UME.LookupMappings lookup definition is used to map each lookup definition with the data source from which values must be fetched for the lookup definition from the target system. The Code Key column of these lookup definitions contains names of the lookup definitions that are synchronized with the target system. The Decode column contains the data source name.

Table 1–2 lists the entries in these lookup definitions. The Decode column holds a list of parameters required to fetch values from each lookup field on the target system.

Table 1–2 Entries in the Lookup.SAP.UME.LookupMappings Lookup Definition

Code Key	Decode
Lookup.SAP.UME.Roles	saprole
Lookup.SAP.UME.Groups	sapgroup

The following is the format of entries in the lookup definitions listed in this table:

- Code Key format: *`IT_RESOURCE_KEY~LOOKUP_FIELD_ID`*

  In this format:

  – *`IT_RESOURCE_KEY`* is the numeric code assigned to the IT resource in Oracle Identity Manager.

  – *`LOOKUP_FIELD_ID`* is the target system code assigned to the lookup field entry.

  Sample value: `1~SAP_EHS_SAF_UTIL`

- Decode format: *`IT_RESOURCE_NAME~LOOKUP_FIELD_ENTRY`*

  In this format:

  – *`IT_RESOURCE_NAME`* is the name of the IT resource in Oracle Identity Manager.

  – *`LOOKUP_FIELD_ENTRY`* is the value or description of the lookup field entry on the target system.

  Sample value: `SAP UME IT Resource~Tools`

The SAP UME Lookup Recon scheduled task is used to synchronize values of these lookup definitions with the target system. Section 3.2, "Scheduled Task for Lookup Field Synchronization" provides more information about this scheduled task.

While performing a provisioning operation on the Administrative and User Console, you select the IT resource for the target system on which you want to perform the operation. When you perform this action, the lookup definitions on the page are automatically populated with values corresponding to the IT resource (target system installation) that you select.

During lookup field synchronization, new entries are appended to the existing set of entries in the lookup definitions. Because the IT resource key is part of each entry created in each lookup definition, only lookup field entries that are specific to the IT resource you select during a provisioning operation are displayed.

1.5.2 Preconfigured Lookup Definitions

Table 1–3 describes the other lookup definitions that are created in Oracle Identity Manager when you deploy the connector. These lookup definitions are either prepopulated with values or values must be manually entered in them after the connector is deployed.

Table 1–3 Preconfigured Lookup Definitions

Lookup Definition	Description of Values	Method to Specify Values for the Lookup Definition
Lookup.SAP.CUP.Configuration	This lookup definition holds connector configuration entries that are used during reconciliation and provisioning by the Compliant User Provisioning feature.	Section 2.3.7.4, "Setting Values in the Lookup.SAP.CUP.Configuration Lookup Definition" describes the entries for which you must set values.
Lookup.SAP.CUP.Constants	This lookup definition stores values that are used internally by the Compliant User Provisioning feature of the connector. The connector development team can use this lookup definition to make minor configuration changes in the connector.	You must not modify the entries in this lookup definition.
Lookup.SAP.CUP.ProvisionAttrMap	This lookup definition holds mappings between process form fields and single-valued attributes on SAP GRC Compliant User Provisioning.	This lookup definition is preconfigured. Table 1–8 lists the default entries in this lookup definition.
Lookup.SAP.CUP.ProvisionRoleAttrMap	This lookup definition holds mappings between process form fields and multivalued attributes on SAP GRC Compliant User Provisioning.	This lookup definition is preconfigured. Table 1–9 lists the default entries in this lookup definition.
Lookup.SAP.UME.Configuration	This lookup definition holds connector configuration entries that are used during reconciliation and provisioning.	Some of the entries in this lookup definition are preconfigured. See Section 2.3.1, "Setting Values in the Lookup.SAP.UME.Configuration Lookup Definition" for information about the entries for which you can set values.
Lookup.SAP.UME.Constants	This lookup definition stores values that are used internally by the connector. The connector development team can use this lookup definition to make minor configuration changes in the connector.	You must not modify the entries in this lookup definition.
Lookup.SAP.UME.ExclusionList	This lookup definition holds user IDs of target system accounts for which you do not want to perform reconciliation and provisioning.	You can enter user IDs in this lookup definition. See Section 2.3.5, "Setting Up the Lookup.SAP.UME.ExclusionList Lookup Definition" for more information.

Table 1–3 (Cont.) Preconfigured Lookup Definitions

Lookup Definition	Description of Values	Method to Specify Values for the Lookup Definition
Lookup.SAP.UME.FullReconFilter	This lookup definition contains the list of characters that can be used in the logon name of an SAP User Management Engine account.	This lookup definition is preconfigured. You must not modify the entries in this lookup definition.
Lookup.SAP.UME.LookupMappings	These lookup definitions hold data required to synchronize other lookup definitions with the target system.	This lookup definition is preconfigured. You must not modify the entries in this lookup definition.
Lookup.SAP.UME.ReconAttrMap	This lookup definition holds mappings between resource object fields and single-valued target system attributes.	This lookup definition is preconfigured. Table 1–4 lists the default entries in this lookup definition.
Lookup.SAP.UME.ReconChildAttrMap	This lookup definition holds mappings between resource object fields and multivalued target system attributes.	This lookup definition is preconfigured. Table 1–5 lists the default entries in this lookup definition.
Lookup.SAP.UME.ReconTransformation	This lookup definition is used to configure transformation of attribute values that are fetched from the target system during user reconciliation.	You manually create entries in this lookup definition. See Section 4.2, "Configuring Transformation of Data During User Reconciliation" for more information.
Lookup.SAP.UME.ReconValidation	This lookup definition is used to configure validation of attribute values that are fetched from the target system during reconciliation.	You manually create entries in this lookup definition. See Section 4.1, "Configuring Validation of Data During Reconciliation and Provisioning" for more information.
Lookup.SAP.UME.System	This lookup definition is used to hold the system IDs of application that use the data source with which SAP User Management Engine is linked.	You manually create entries in this lookup definition. See Section 2.3.6, "Setting Up the Lookup.SAP.UME.System Lookup Definition" for more information.

1.6 Connector Objects Used During Reconciliation

The SAP UME User Recon scheduled task is used to initiate a reconciliation run. This scheduled task is discussed in Section 3.5.3, "Reconciliation Scheduled Tasks".

> **See Also:** The "Reconciliation" section in *Oracle Identity Manager Connector Concepts* for conceptual information about reconciliation

This section discusses the following topics:

- Section 1.6.1, "User Attributes for Reconciliation"
- Section 1.6.2, "Reconciliation Rules"
- Section 1.6.3, "Reconciliation Action Rules"

1.6.1 User Attributes for Reconciliation

The Lookup.SAP.UME.ReconAttrMap lookup definition maps process form fields and target system attributes. The Code Key column stores the names of attributes in the SPML schema and the Decode column stores the labels of the process form fields.

Table 1–4 lists entries in this lookup definition.

Table 1–4 Entries in the Lookup.SAP.UME.ReconAttrMap Lookup Definition

Target System Attribute	Process Form Label
email	E Mail
salutation	Salutation
title	Title
jobtitle	Job Title
mobile	Mobile
telephone	Telephone Number
fax	Fax Number
locale	Locale
timezone	Time Zone
department	Department
logonname	User ID
firstname	First Name
lastname	Last Name
validto	Valid Through
validfrom	Valid From

The Lookup.SAP.UME.ReconChildAttrMap lookup definition maps resource object fields and multivalued target system attributes. The Code Key column stores the names of attributes in the SPML schema, and the Decode column stores the names of reconciliation fields in the resource object.

Table 1–5 lists entries in this lookup definition.

Table 1–5 Entries in the Lookup.SAP.UME.ReconChildAttrMap Lookup Definition

Target System Attribute	Reconciliation Field
assignedroles	RoleName
assignedgroups	GroupName

1.6.2 Reconciliation Rules

> **See Also:** *Oracle Identity Manager Connector Concepts* for generic information about reconciliation matching and action rules

The following sections provide information about the reconciliation rules for this connector:

- Section 1.6.2.1, "Reconciliation Rule"
- Section 1.6.2.2, "Viewing Reconciliation Rules in the Design Console"

1.6.2.1 Reconciliation Rule

The following is the process-matching rule:

Rule name: SAP UME Recon Rule

Rule element: User Login Equals User ID

In this rule element:

- User Login is the User ID field of the OIM User form.
- User ID is the user ID of the SAP account.

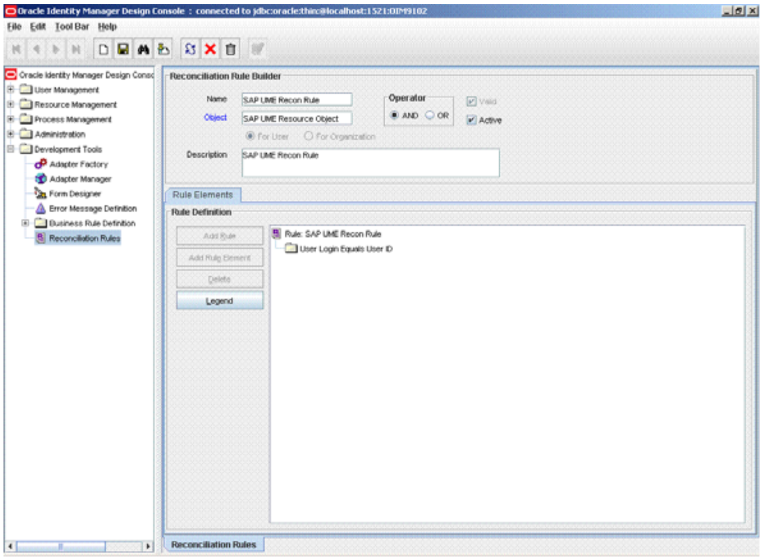
1.6.2.2 Viewing Reconciliation Rules in the Design Console

After you deploy the connector, you can view the reconciliation rule for reconciliation by performing the following steps:

> **Note:** Perform the following procedure only after the connector is deployed.

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for and open the **SAP UME Recon Rule** rule. Figure 1–2 shows this reconciliation rule.

Figure 1–2 Reconciliation Rule



Name: SAP UME Recon Rule

Object: SAP UME Resource Object

Operator: ● AND ○ OR

☑ Valid

☑ Active

● For User ○ For Organization

Description: SAP UME Recon Rule

Rule: SAP UME Recon Rule

User Login Equals User ID

1.6.3 Reconciliation Action Rules

> **Note:** No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. See *Oracle Identity Manager Design Console Guide* for information about modifying or creating reconciliation action rules.

The following sections provide information about the reconciliation rules for this connector:

- Section 1.6.3.1, "Reconciliation Action Rules for Reconciliation"
- Section 1.6.3.2, "Viewing Reconciliation Action Rules in the Design Console"

1.6.3.1 Reconciliation Action Rules for Reconciliation

Table 1–6 lists the action rules for reconciliation.

Table 1–6 Action Rules for Reconciliation

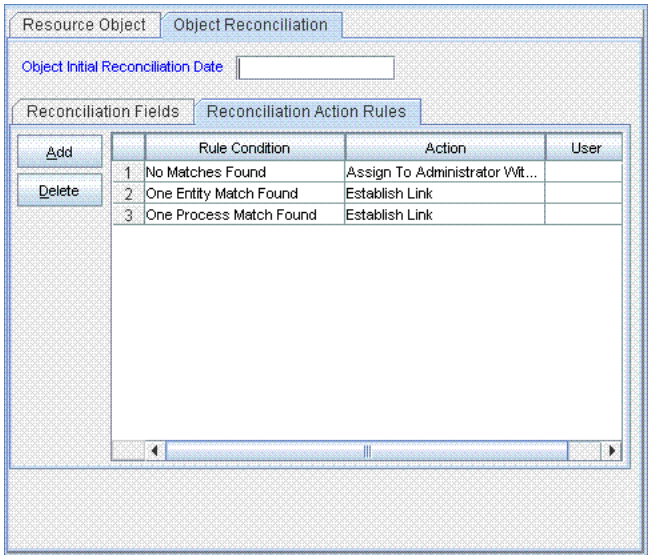
Rule Condition	Action
No Matches Found	Assign to Administrator With Least Load
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

1.6.3.2 Viewing Reconciliation Action Rules in the Design Console

After you deploy the connector, you can view the reconciliation action rules for reconciliation by performing the following steps:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**, and double-click **Resource Objects**.
3. If you want to view the reconciliation action rules for reconciliation, then search for and open the **SAP UME Resource Object** resource object.
4. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1–3 shows the reconciliation action rules for reconciliation.

Figure 1–3 Reconciliation Action Rules



	Rule Condition	Action	User
1	No Matches Found	Assign To Administrator Wit...	
2	One Entity Match Found	Establish Link	
3	One Process Match Found	Establish Link	

1.7 Connector Objects Used During Provisioning

Provisioning involves creating or modifying user data on the target system through Oracle Identity Manager.

See Also: The "Provisioning" section in *Oracle Identity Manager Connector Concepts* for conceptual information about provisioning

This section discusses the following topics:

- Section 1.7.1, "User Provisioning Functions"
- Section 1.7.2, "User Attributes for Provisioning"

1.7.1 User Provisioning Functions

Table 1–7 lists the supported user provisioning functions and the adapters that perform these functions. The functions listed in the table correspond to either a single or multiple process tasks.

See Also: *Oracle Identity Manager Connector Concepts* for generic information about process tasks and adapters

Table 1–7 User Provisioning Functions

Function	Adapter
Create a user account	UME Create User
Update a user account	UME Modify User
Delete a user account	UME Delete User
Lock or unlock a user account	UME Lock UnLock User
Enable a user account	UME Enable User
Disable a user account	UME Disable User
Change the password of an account	UME Modify Password
Add (provision) a multivalued attribute (for example, role or group)	UME Add Multivalue Data
Remove (revoke) a multivalued attribute (for example, role or group)	UME Remove Multivalue Data
Update a multivalued attribute (for example, role or group)	UME Update Multivalue Data

1.7.2 User Attributes for Provisioning

In the Compliant User Provisioning feature, the Lookup.SAP.CUP.ProvAttrMap lookup definition maps process form fields with single-valued attributes in SAP GRC Compliant User Provisioning. Table 1–8 lists entries in this lookup definition.

Table 1–8 Entries in the Lookup.SAP.CUP.ProvAttrMap Lookup Definition

Process Form Field	Target System Attribute
CUP Requestor ID	requestorId;TEXT;STANDARD;NONE;MANDATORY
CUP Requestor First Name	requestorFirstName;TEXT;STANDARD;NONE;MANDATORY
CUP Requestor Last Name	requestorLastName;TEXT;STANDARD;NONE;MANDATORY
CUP Requestor Email	requestorEmailAddress;TEXT;STANDARD;NONE;MANDATORY
E Mail	emailAddress;TEXT;STANDARD;E_MAIL;MANDATORY
First Name	firstName;TEXT;STANDARD;FIRSTNAME;MANDATORY

Table 1–8 (Cont.) Entries in the Lookup.SAP.CUP.ProvAttrMap Lookup Definition

Process Form Field	Target System Attribute
Last Name	lastName;TEXT;STANDARD;LASTNAME;MANDATORY
User ID	userId;TEXT;STANDARD;NONE;MANDATORY
Valid From	validFrom;DATE;STANDARD;GLTGV;NONE
Valid Through	validTo;DATE;STANDARD;GLTGB;MANDATORY

In the Compliant User Provisioning feature, the Lookup.SAP.CUP.ProvisionRoleAttrMap lookup definition maps process form fields with multivalued attributes (roles and profiles) in SAP GRC Compliant User Provisioning. Table 1–9 lists entries in this lookup definition.

Table 1–9 Entries in the Lookup.SAP.CUP.ProvisionRoleAttrMap Lookup Definition

Process Form Field	Target System Attribute
Role Name	roleId;LOOKUP
Group Name	roleId;LOOKUP

1.8 Roadmap for Deploying and Using the Connector

The following is the organization of information in the rest of this guide:

- Chapter 2, "Deploying the Connector" describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.
- Chapter 3, "Using the Connector" describes guidelines on using the connector and the procedure to configure reconciliation runs and perform provisioning operations.
- Chapter 4, "Extending the Functionality of the Connector" describes the procedures to perform if you want to extend the functionality of the connector.
- Chapter 5, "Known Issues and Limitations" lists known issues and limitations associated with this release of the connector.

2 Deploying the Connector

The procedure to deploy the connector can be divided into the following stages:

- Section 2.1, "Preinstallation"
- Section 2.2, "Installation"
- Section 2.3, "Postinstallation"

> **Note:** Some of the procedures described in this chapter must be performed on the target system. To perform these procedures, you must use an SAP administrator account to which the SAP_ALL and SAP_NEW profiles have been assigned.

2.1 Preinstallation

Preinstallation information is divided across the following sections:

- Section 2.1.1, "Preinstallation on Oracle Identity Manager"
- Section 2.1.2, "Preinstallation on the Target System"

2.1.1 Preinstallation on Oracle Identity Manager

This section contains the following topics:

- Section 2.1.1.1, "Files and Directories on the Installation Media"
- Section 2.1.1.2, "Determining the Release Number of the Connector"
- Section 2.1.1.3, "Creating a Backup of the Existing Common.jar File"
- Section 2.1.1.4, "Copying OpenSPML Toolkit 2.0"

2.1.1.1 Files and Directories on the Installation Media

Table 2–1 describes the files and directories on the installation media.

Table 2–1 Files and Directories On the Installation Media

File in the Installation Media Directory	Description
configuration/SAPUME-CI.xml	This XML file contains configuration information that is used during connector installation.
deploy/SAPCUP.jar	This JAR file contains class files that are used when you configure the Compliant User Provisioning feature.
lib/SAPUME.jar	This JAR file contains the class files that are used in connector operations. During connector deployment, this file is copied into the following directory: *OIM_HOME*/xellerate/JavaTasks
lib/SAPCommon.jar	This JAR file contains the class files that are common to all SAP connectors. During connector deployment, this file is copied into the following directory: *OIM_HOME*/xellerate/ScheduleTask
lib/Common.jar	This JAR file contains the class files that are common to all connectors. During connector deployment, this file is copied into the following directory: *OIM_HOME*/xellerate/ScheduleTask
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector deployment, this file is copied into the following directory: *OIM_HOME*/xellerate/connectorResources **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.
xml/SAP-UME-Main-ConnectorConfig.xml	This XML file contains definitions of connector objects.

2.1.1.2 Determining the Release Number of the Connector

You might have a deployment of an earlier release of the connector. While deploying the latest release, you might want to know the release number of the earlier release. To determine the release number of the connector that has already been deployed:

1. In a temporary directory, extract the contents of the connector JAR file that is in the *OIM_HOME*/xellerate/JavaTasks directory.
2. Open the Manifest.mf file in a text editor. The Manifest.mf file is one of the files bundled inside the connector JAR file.

   In the Manifest.mf file, the release number of the connector is displayed as the value of the Version property.

2.1.1.3 Creating a Backup of the Existing Common.jar File

The Common.jar file is in the deployment package of each release 9.1.x connector. With each new release, code corresponding to that particular release is added to the existing code in this file. For example, the Common.jar file shipped with Connector Y on 12-July contains:

- Code specific to Connector Y
- Code included in the Common.jar files shipped with all other release 9.1.x connectors that were released before 12-July.

If you have already installed a release 9.1.x connector that was released after this release of the SAP User Management Engine connector, back up the existing

Common.jar file, install the SAP User Management Engine connector, and then restore the Common.jar file. The steps to perform this procedure are as follows:

> **Caution:** If you do not perform this procedure, then your release 9.1.x connectors might not work.

1. Determine the release date of your existing release 9.1.x connector as follows:

   a. Extract the contents of the following file in a temporary directory:

      OIM_HOME/xellerate/ScheduleTask/Common.jar

   b. Open the Manifest.mf file in a text editor.

   c. Note down the Build Date and Build Version values.

2. Determine the release date of this connector as follows:

   a. On the installation media for the connector, extract the contents of the lib/Common.jar and then open the Manifest.mf file in a text editor.

   b. Note down the Build Date and Build Version values.

3. If the Build Date and Build Version values for the SAP User Management Engine connector are less than the Build Date and Build Version values for the connector that is already installed, then:

   a. Copy the *OIM_HOME*/xellerate/ScheduleTask/Common.jar to a temporary location.

   b. After you perform the procedure described in Section 2.2, "Installation" overwrite the new Common.jar file in the *OIM_HOME*/xellerate/ScheduleTask directory with the Common.jar file that you backed up in the preceding step.

2.1.1.4 Copying OpenSPML Toolkit 2.0

The connector uses OpenSPML Toolkit 2.0. To download this toolkit:

1. In a Web browser, open the following Web page:

   `https://openspml.dev.java.net/downloads.html`

2. Download the SPMLv2 build 192-20100413 file.

3. Extract the openspml2-toolkit.jar file from the downloaded file.

4. Copy the openspml2-toolkit.jar file into the *OIM_HOME*/xellerate/ThirdParty directory.

2.1.2 Preinstallation on the Target System

Preinstallation on the target system involves performing the following procedure:

- Section 2.1.2.1, "Creating a Target System User Account for Connector Operations"

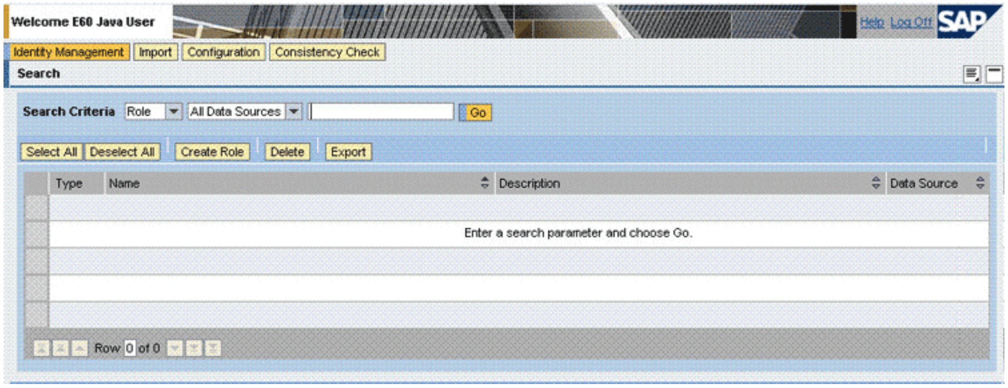
2.1.2.1 Creating a Target System User Account for Connector Operations

The connector uses a target system account to connect to and perform operations on the target system. To create this target system account:

1. Log in to SAP User Management Engine as the administrator.

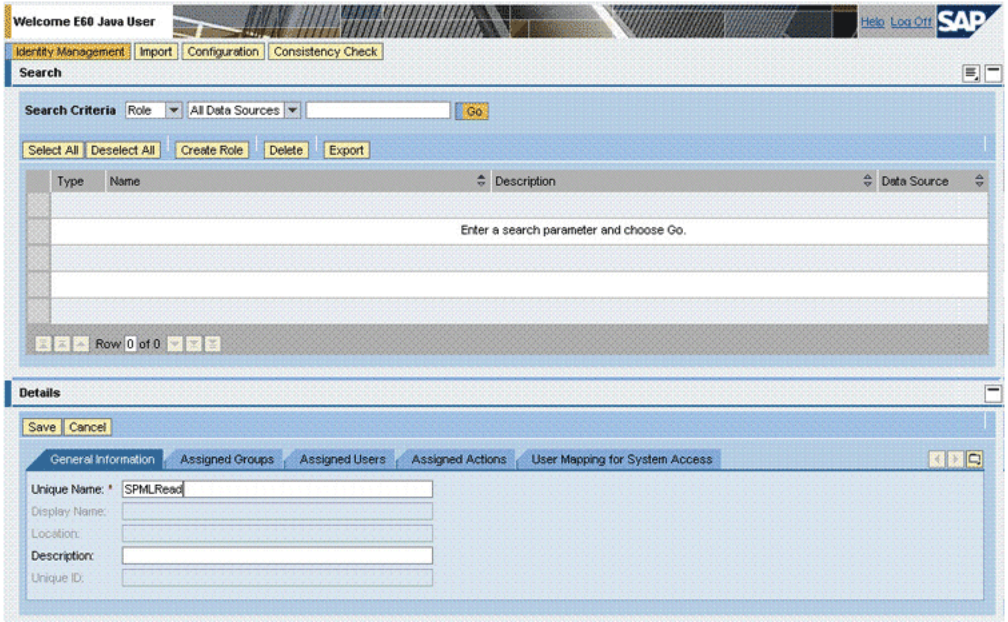
2. Create a role and assign the Spml_Read_Action action to it as follows:

a. From the Search Criteria list, select **Role** and then click **Create Role**.



Enter a search parameter and choose Go.

b. On the General Information tab of the Details region, enter a name for the role in the **Unique Name** field and then click **Save**.



Enter a search parameter and choose Go.

Unique Name: * SPMLRead

Display Name:

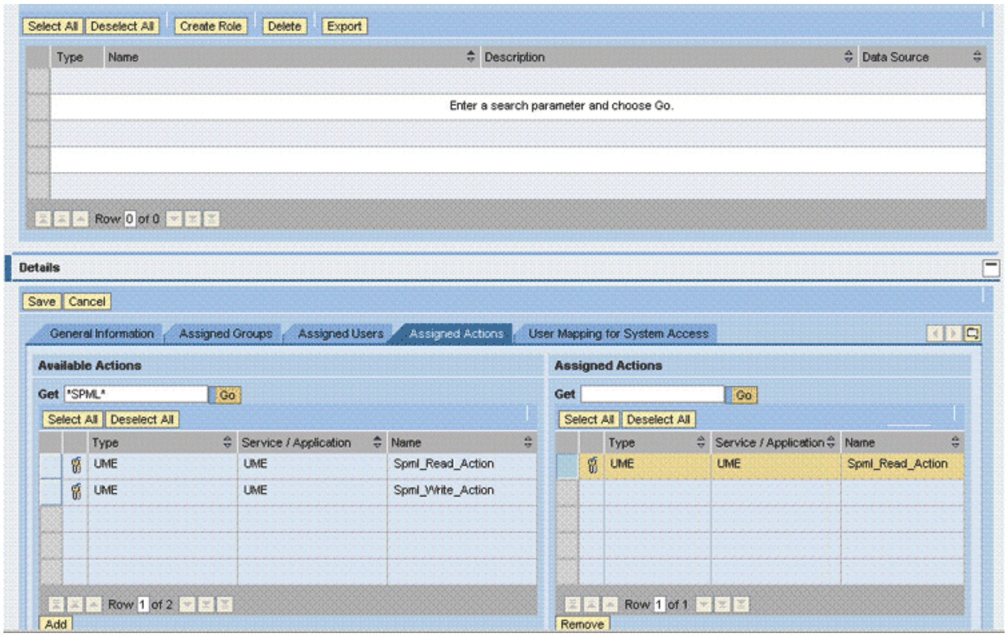
Location:

Description:

Unique ID:

c. On the Assigned Actions tab, use the **Get** field to display the **Spml_Read_Action** action, select this action, and then click **Add**.

The Spml_Read_Action action is displayed in the Assigned Actions list.



Type	Name	Description	Data Source
Enter a search parameter and choose Go.			

Get *SPML*

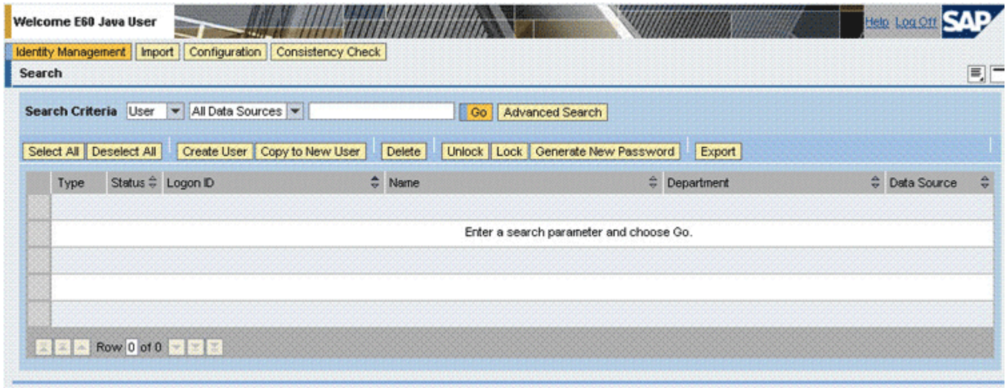
Type	Service / Application	Name
UME	UME	Spml_Read_Action
UME	UME	Spml_Write_Action

Type	Service / Application	Name
UME	UME	Spml_Read_Action

d. Click **Save** in the Details region.

3. Create a user and assign the newly created role to the user as follows:

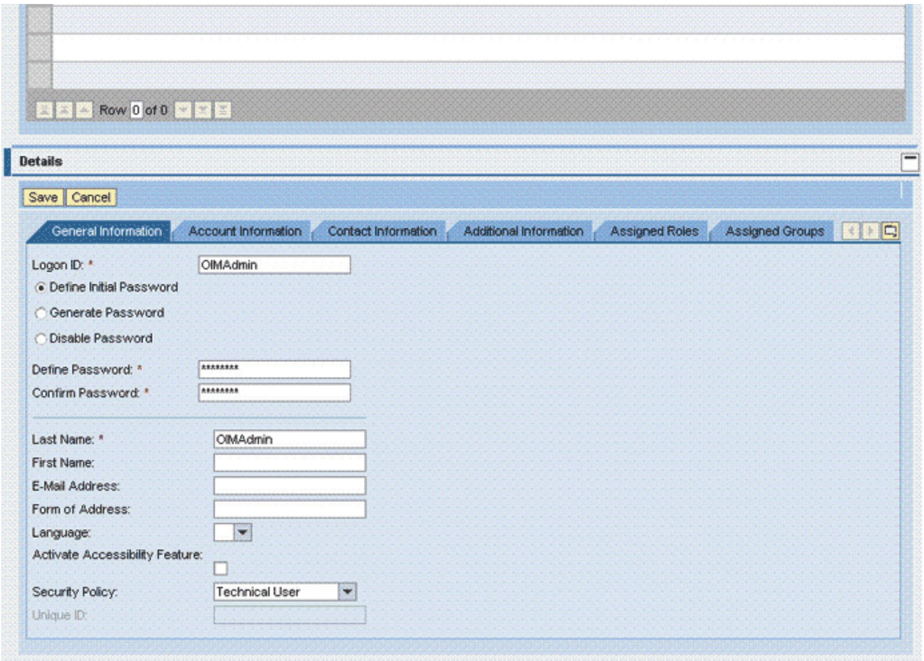
a. From the Search Criteria list, select **User** and then click **Create User**.



Search Criteria User All Data Sources

Type	Status	Logon ID	Name	Department	Data Source
Enter a search parameter and choose Go.					

b. On the General Information tab of the Details region, enter values in the various fields and then select **Technical User** from the Security Policy list.



Logon ID: * OIMAdmin

● Define Initial Password

○ Generate Password

○ Disable Password

Define Password: * ********

Confirm Password: * ********

Last Name: * OIMAdmin

First Name:

E-Mail Address:

Form of Address:

Language:

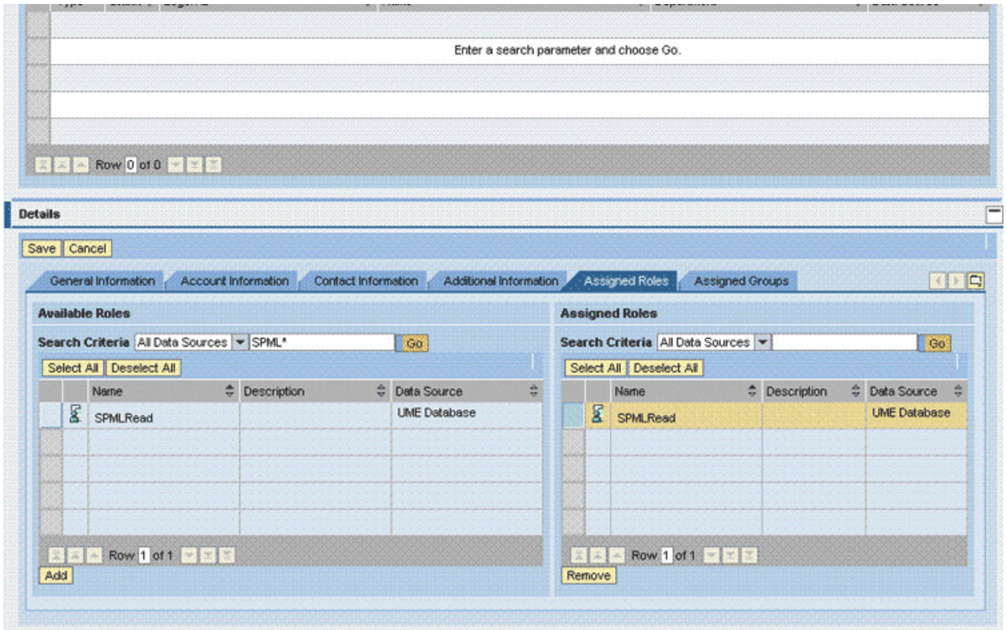
Activate Accessibility Feature: □

Security Policy: Technical User

Unique ID:

c. Click **Save** in the Details region.

d. On the Assigned Roles tab, assign the newly created role to the user and then click **Save**.



Enter a search parameter and choose Go.

Available Roles

Search Criteria All Data Sources SPML*

Name	Description	Data Source
SPMLRead		UME Database

Row 1 of 1

Assigned Roles

Search Criteria All Data Sources

Name	Description	Data Source
SPMLRead		UME Database

Row 1 of 1

2.2 Installation

Note: In this guide, the term **Connector Installer** has been used to refer to the Connector Installer feature of the Oracle Identity Manager Administrative and User Console.

To run the Connector Installer:

1. Copy the contents of the connector installation media into the following directory:

   OIM_HOME/xellerate/ConnectorDefaultDirectory

2. Log in to the Administrative and User Console by using the user account described in the "Creating the User Account for Installing Connectors" section of *Oracle Identity Manager Administrative and User Console*.

3. Click **Deployment Management**, and then click **Install Connector**.

4. From the Connector List list, select **SAP UME** ***RELEASE_NUMBER***. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory:

   OIM_HOME/xellerate/ConnectorDefaultDirectory

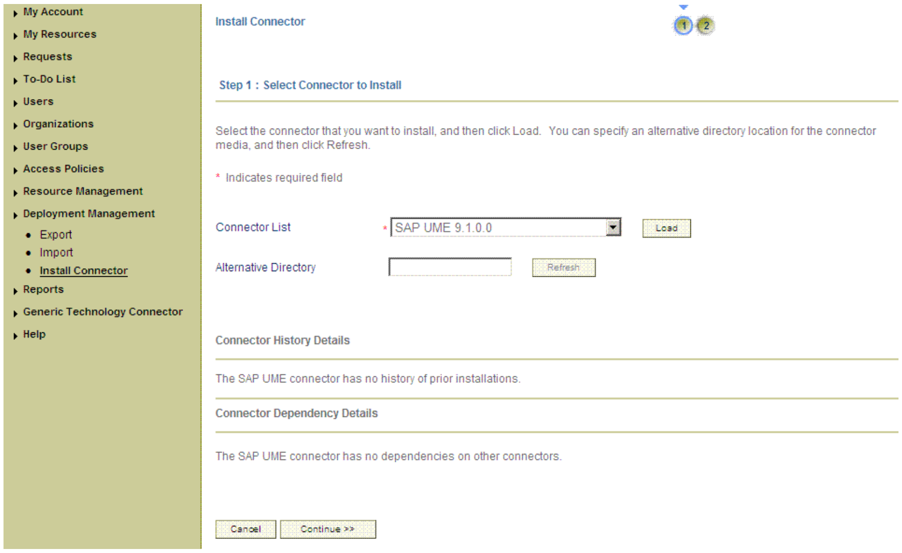
   If you have copied the installation files into a different directory, then:

   a. In the **Alternative Directory** field, enter the full path and name of that directory.

   b. To repopulate the list of connectors in the Connector List list, click **Refresh**.

   c. From the Connector List list, select **SAP UME** ***RELEASE_NUMBER***.

5. Click **Load**. The following screenshot shows this page:



Install Connector

Step 1 : Select Connector to Install

Select the connector that you want to install, and then click Load. You can specify an alternative directory location for the connector media, and then click Refresh.

* Indicates required field

Connector List * SAP UME 9.1.0.0

Alternative Directory

Connector History Details

The SAP UME connector has no history of prior installations.

Connector Dependency Details

The SAP UME connector has no dependencies on other connectors.

6. To start the installation process, click **Continue**.

   The following tasks are performed in sequence:

   a. Configuration of connector libraries

   b. Import of the connector XML files (by using the Deployment Manager)

   c. Compilation of adapters

   On successful completion of a task, a check mark is displayed for the task. If a task fails, then an X mark and a message stating the reason for failure are displayed. If a task fails, then make the required correction and perform one of the following steps:

   - Retry the installation by clicking **Retry.**

- Cancel the installation and begin again from Step 3.

7. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed.

   In addition, a list of the steps that you must perform after the installation is displayed. These steps are as follows:

   a. Ensuring that the prerequisites for using the connector are addressed

   > **Note:** At this stage, run the PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. See Section 2.3.3, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for information about running the PurgeCache utility.
   >
   > There are no prerequisites for some predefined connectors.

   b. Configuring the IT resource for the connector

   Record the name of the IT resource displayed on this page. The procedure to configure the IT resource is described later in this guide.

   c. Configuring the scheduled tasks that are created when you installed the connector

   Record the names of the scheduled tasks displayed on this page. The procedure to configure these scheduled tasks is described later in this guide.

8. Restart Oracle Identity Manager.

> **Note:** When you run the Connector Installer, it copies the connector files and external code files to destination directories on the Oracle Identity Manager host computer. These files are listed in Table 2–1.

Installing the Connector in an Oracle Identity Manager Cluster

While installing Oracle Identity Manager in a clustered environment, you must copy all the JAR files and the contents of the connectorResources directory into the corresponding directories on each node of the cluster. Then, restart each node. See Section 2.1.1.1, "Files and Directories on the Installation Media" for information about the files that you must copy and their destination locations on the Oracle Identity Manager server.

Restoring the Common.jar File

If required, restore the Common.jar file that you had backed up by following the procedure described in Section 2.1.1.3, "Creating a Backup of the Existing Common.jar File".

2.3 Postinstallation

Postinstallation steps are divided across the following sections:

- Section 2.3.1, "Setting Values in the Lookup.SAP.UME.Configuration Lookup Definition"
- Section 2.3.2, "Changing to the Required Input Locale"

- Section 2.3.3, "Clearing Content Related to Connector Resource Bundles from the Server Cache"
- Section 2.3.4, "Enabling Logging"
- Section 2.3.5, "Setting Up the Lookup.SAP.UME.ExclusionList Lookup Definition"
- Section 2.3.6, "Setting Up the Lookup.SAP.UME.System Lookup Definition"
- Section 2.3.7, "Configuring the Compliant User Provisioning Feature of the Connector"
- Section 2.3.8, "Configuring SSL to Secure Communication Between the Target System and Oracle Identity Manager"
- Section 2.3.9, "Configuring the IT Resource"

2.3.1 Setting Values in the Lookup.SAP.UME.Configuration Lookup Definition

Table 2–2 describes the entries in the Lookup.SAP.UME.Configuration lookup definition.

> **Note:** You must not change any of the Code Key values of this lookup definition.

Table 2–2 Entries in the Lookup.SAP.UME.Configuration Lookup Definition

Code Key	Description
Constants Lookup	This entry holds the name of the lookup definition that stores values used by the connector. The connector development team can use this lookup definition to make minor configuration changes in the connector. Value: `Lookup.SAP.UME.Constants`
CUP Configuration Lookup	This entry holds the name of the lookup definition that stores configuration values for the Compliant User Provisioning feature. Value: `Lookup.SAP.CUP.Configuration`
Exclusion List Lookup	This entry holds the name of the lookup definition in which you enter user IDs of target system accounts for which you do not want to perform reconciliation and provisioning. See Section 2.3.5, "Setting Up the Lookup.SAP.UME.ExclusionList Lookup Definition" for more information. Value: `Lookup.SAP.UME.ExclusionList`
Transform Lookup For Recon	This entry holds the name of the lookup definition that you can use to configure transformation of attribute values fetched from the target system during reconciliation. See Section 4.2, "Configuring Transformation of Data During User Reconciliation" for more information. Value: `Lookup.SAP.UME.ReconTransformation`
Use Transformation For Recon	Enter `yes` if you want to configure transformation of attribute values fetched from the target system during reconciliation. See Section 4.2, "Configuring Transformation of Data During User Reconciliation" for more information. Default value: `no`

Table 2–2 (Cont.) Entries in the Lookup.SAP.UME.Configuration Lookup Definition

Code Key	Description
Use Validation For Prov	Enter yes if you want to configure validation of attribute values entered on the process form during provisioning operations. See Section 4.1, "Configuring Validation of Data During Reconciliation and Provisioning" for more information. Default value: `no`
Use Validation For Recon	Enter `yes` if you want to configure validation of attribute values that are fetched from the target system during reconciliation. See Section 4.1, "Configuring Validation of Data During Reconciliation and Provisioning" for more information. Default value: `no`
Validation Lookup For Prov	This entry holds the name of the lookup definition that you can use to configure validation of attribute values entered on the process form during provisioning operations. See Section 4.1, "Configuring Validation of Data During Reconciliation and Provisioning" for more information. Value: `Lookup.SAP.UME.ProvValidation`
Validation Lookup For Recon	This entry holds the name of the lookup definition that you can use to configure validation of attribute values entered on the process form during reconciliation. See Section 4.1, "Configuring Validation of Data During Reconciliation and Provisioning" for more information. Value: `Lookup.SAP.UME.ReconValidation`

2.3.2 Changing to the Required Input Locale

Note: In a clustered environment, perform this procedure on each node of the cluster. Then, restart each node.

Changing to the required input locale (language and country setting) involves installing the required fonts and setting the required input locale.

You may require the assistance of the system administrator to change to the required input locale.

2.3.3 Clearing Content Related to Connector Resource Bundles from the Server Cache

Note: In a clustered environment, perform this procedure on each node of the cluster. Then, restart each node.

During the connector deployment procedure, files are copied from the resources directory on the installation media into the *OIM_HOME*/xellerate/connectorResources directory. Whenever you add a new resource bundle in the connectorResources directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

To clear content related to connector resource bundles from the server cache:

1. In a command window, change to the *OIM_HOME*/xellerate/bin directory.

Note: You must perform Step 1 before you perform Step 2. An exception is thrown if you run the command described in Step 2 as follows:

OIM_HOME/xellerate/bin/*batch_file_name*

2. Enter one of the following commands:

   - On Microsoft Windows:

     ```
     PurgeCache.bat ConnectorResourceBundle
     ```

   - On UNIX:

     ```
     PurgeCache.sh ConnectorResourceBundle
     ```

   Note: You can ignore the exception that is thrown when you perform Step 2.

   In this command, ConnectorResourceBundle is one of the content categories that you can remove from the server cache. Refer to the following file for information about the other content categories:

   OIM_HOME/xellerate/config/xlConfig.xml

2.3.4 Enabling Logging

Note: In a clustered environment, perform this procedure on each node of the cluster. Then, restart each node.

When you enable logging, Oracle Identity Manager automatically stores in a log file information about events that occur during the course of provisioning and reconciliation operations. To specify the type of event for which you want logging to take place, you can set the log level to one of the following:

- ALL

  This level enables logging for all events.

- DEBUG

  This level enables logging of information about fine-grained events that are useful for debugging.

- INFO

  This level enables logging of messages that highlight the progress of the application at a coarse-grained level.

- WARN

  This level enables logging of information about potentially harmful situations.

- ERROR

  This level enables logging of information about error events that may allow the application to continue running.

- FATAL

This level enables logging of information about very severe error events that could cause the application to stop functioning.

- OFF

  This level disables logging for all events.

The file in which you set the log level and the log file path depend on the application server that you use:

- **IBM WebSphere Application Server**

  To enable logging:

  1. Add the following lines in the *OIM_HOME*/xellerate/config/log.properties file:

     ```
     log4j.logger.XELLERATE=log_level
     log4j.logger.OIMCP.SAPU=log_level
     ```

  2. In these lines, replace `log_level` with the log level that you want to set.

     For example:

     ```
     log4j.logger.XELLERATE=INFO
     log4j.logger.OIMCP.SAPU=INFO
     ```

  After you enable logging, log information is written to the following file:

  WEBSPHERE_HOME/AppServer/logs/*SERVER_NAME*/SystemOut.log

- **JBoss Application Server**

  To enable logging:

  1. In the *JBOSS_HOME*/server/default/conf/jboss-log4j.xml file, locate or add the following lines if they are not already present in the file:

     ```
     <category name="XELLERATE">
        <priority value="log_level"/>
     </category>

     <category name="OIMCP.SAPU">
        <priority value="log_level"/>
     </category>
     ```

  2. In the second XML code line of each set, replace `log_level` with the log level that you want to set. For example:

     ```
     <category name="XELLERATE">
        <priority value="INFO"/>
     </category>

     <category name="OIMCP.SAPU">
        <priority value="INFO"/>
     </category>
     ```

  After you enable logging, log information is written to the following file:

  JBOSS_HOME/server/default/log/server.log

- **Oracle Application Server**

  To enable logging:

  1. Add the following lines in the *OIM_HOME*/xellerate/config/log.properties file:

```
log4j.logger.XELLERATE=log_level
log4j.logger.OIMCP.SAPU=log_level
```

2. In these lines, replace `log_level` with the log level that you want to set.

   For example:

```
log4j.logger.XELLERATE=INFO
log4j.logger.OIMCP.SAPU=INFO
```

After you enable logging, log information is written to the following file:

ORACLE_HOME/opmn/logs/default_group~home~default_group~1.log

- **Oracle WebLogic Server**

  To enable logging:

  1. Add the following lines in the *OIM_HOME*/xellerate/config/log.properties file:

```
log4j.logger.XELLERATE=log_level
log4j.logger.OIMCP.SAPU=log_level
```

  2. In these lines, replace `log_level` with the log level that you want to set.

     For example:

```
log4j.logger.XELLERATE=INFO
log4j.logger.OIMCP.SAPU=INFO
```

  After you enable logging, the log information is written to the following file:

  WEBLOGIC_HOME/user_projects/domains/*DOMAIN_NAME*/*SERVER_NAME* /*SERVER_NAME*.log

2.3.5 Setting Up the Lookup.SAP.UME.ExclusionList Lookup Definition

> **Note:** In a clustered environment, perform this procedure on each node of the cluster. Then, restart each node.

In the Lookup.SAP.UME.ExclusionList lookup definition, enter the user IDs of target system accounts for which you do not want to perform reconciliation and provisioning:

1. On the Design Console, expand **Administration** and then double-click **Lookup Definition**.
2. Search for and open the **Lookup.SAP.UME.ExclusionList** lookup definition.
3. Click **Add**.
4. In the Code Key and Decode columns, enter the first user ID that you want to exclude. You must enter the same value in both columns.

   > **Note:** You must enter the user ID in the same case (uppercase and lowercase) in which it is stored on the target system.

5. Repeat Steps 3 and 4 for all the user IDs that you want to exclude.

6. Click the Save icon.

2.3.6 Setting Up the Lookup.SAP.UME.System Lookup Definition

The Lookup.SAP.UME.System lookup definition is used to hold system IDs of applications that use the data source with which SAP User Management Engine is linked. To create entries in this lookup definition:

1. On the Design Console, expand **Administration** and then double-click **Lookup Definition**.
2. Search for and open the **Lookup.SAP.UME.System** lookup definition.
3. Click **Add**.
4. In the **Code** and **Decode** columns, enter the system ID of the application.
5. Repeat Steps 3 and 4 to create entries for the remaining applications that use the data source.
6. Click the Save icon.

2.3.7 Configuring the Compliant User Provisioning Feature of the Connector

Oracle Identity Manager can be configured as the medium for sending provisioning requests to SAP GRC Compliant User Provisioning. A request from Oracle Identity Manager is sent to Compliant User Provisioning, which forwards the provisioning data contained within the request to the target system. The outcome is the creation of or modification to the user's account on the target system.

The following sections provide information about configuring the Compliant User Provisioning feature:

- Section 2.3.7.1, "Specifying Values for the SAP GRC IT Resource IT Resource"
- Section 2.3.7.2, "Setting Up the Link with the Web Services for SAP GRC Compliant User Provisioning"
- Section 2.3.7.3, "Configuring Request Types and Workflows on SAP GRC Compliant User Provisioning,"
- Section 2.3.7.4, "Setting Values in the Lookup.SAP.CUP.Configuration Lookup Definition,"

2.3.7.1 Specifying Values for the SAP GRC IT Resource IT Resource

The SAP GRC IT Resource IT resource holds information that is used during communication with SAP GRC Compliant User Provisioning. To set values for the parameters of this IT resource:

1. Log in to the Administrative and User Console.
2. Expand **Resource Management.**
3. Click **Manage IT Resource**.
4. In the IT Resource Name field on the Manage IT Resource page, enter `SAP GRC IT Resource` and then click **Search**.
5. Click the edit icon for the IT resource.
6. From the list at the top of the page, select **Details and Parameters**.
7. Specify values for the parameters of the IT resource. Table 2–3 describes each parameter.

Note: Entries in this table are sorted in alphabetical order of parameter names.

Table 2–3 Parameters of the SAP GRC IT Resource IT Resource

Parameter	Description
dbuser	You need not enter a value for this parameter.
dbpassword	You need not enter a value for this parameter.
jdbcURL	Enter the JDBC URL for connecting to the database used by SAP GRC. Sample value: `jdbc:oracle:thin:@10.123.123.123`
password	Enter the password of the account created on SAP GRC for API calls.
port	Enter the number of the port at which SAP GRC is listening. Sample value: `8090`
server	Enter the IP address of the host computer on which SAP GRC is running. Sample value: `10.231.231.231`
Source Datastore Name	You need not enter a value for this parameter.
sslEnable	Enter `true` if SAP GRC accepts only HTTPS communication requests. Otherwise, enter `false`. Sample value: `false`
username	Enter the user name of an account created on SAP GRC. This account is used to call SAP GRC APIs that are used during request validation. Sample value: `jdoe`

8. To save the values, click **Update**.

2.3.7.2 Setting Up the Link with the Web Services for SAP GRC Compliant User Provisioning

To set up the link with the Web services for SAP GRC Compliant User Provisioning:

1. Search for and download the axis-bin-1_4.zip file from the following Web site:

   `http://www.apache.org`

2. Extract the contents of the axis2-1.4-bin.zip file to a temporary directory.
3. The following files are in the *TEMPORARY_DIRECTORY*/axis-1_4/lib directory:

   wsdl4j-1.5.1.jar

   axis.jar

   jaxrpc.jar

   saaj.jar

   commons-discovery-0.2.jar

   commons-logging-1.0.4.jar

   Copy these JAR files into the *OIM_HOME*/xellerate/ext directory and one of the following directories:

   - For IBM Websphere Application Server: *WEBSPHERE_HOME*/lib
   - For JBoss Application Server: *JBOSS_HOME*/server/default/lib

  - For Oracle Application Server: *ORACLE_HOME*/j2ee/home/lib
  - For Oracle WebLogic Server: *WEBLOGIC_DOMAIN_HOME*/lib

4. Copy the deploy/SAPCUP.jar file from the installation media to one of the directories mentioned in the preceding step. If you are using Oracle WebLogic Server, then you must also copy the SAPCUP.jar file to the *WEBLOGIC_HOME*/wlserver_10.3/server/lib directory.
5. If Oracle Identity Manager is running on Oracle Application Server, then perform the following additional steps:

   a. In the temporary directory, extract the contents of the *ORACLE_HOME*/j2ee/home/oc4j.jar file.

   b. In a text editor, open the boot.xml file. This file is bundled in the oc4j.jar file.

   c. In the boot.xml file, add the following lines under the <system-class-loader> tag:

   ```
   <code-source path="lib/wsdl4j-1.5.1.jar"/>
   <code-source path="lib/log4j-1.2.8.jar"/>
   <code-source path="lib/saaj.jar"/>
   <code-source path="lib/axis.jar"/>
   <code-source path="lib/commons-discovery-0.2.jar"/>
   <code-source path="lib/commons-logging-1.0.4.jar"/>
   <code-source path="lib/jaxrpc.jar"/>
   <code-source path="lib/SAPCUP.jar"/>
   ```

   d. Save and close the boot.xml file.

   e. Re-create the oc4j.jar file with the updated boot.xml file bundled inside.

   f. Copy the log4j-1.2.8.jar file from the *OIM_HOME*/xellerate/ext directory into the *ORACLE_HOME*/j2ee/home/lib directory.

2.3.7.3 Configuring Request Types and Workflows on SAP GRC Compliant User Provisioning

You must create and configure request types and workflows on SAP GRC Compliant User Provisioning for provisioning operations.

The following sections describe these procedures in detail:

- Section 2.3.7.3.1, "Creating Request Types"
- Section 2.3.7.3.2, "Creating Workflows"

2.3.7.3.1 Creating Request Types

In SAP GRC Compliant User Provisioning, a request type defines the action that is performed when a request is processed. Oracle Identity Manager is a requester. It works with request types defined in SAP GRC Compliant User Provisioning. The Lookup.SAP.CUP.Configuration lookup definition maps request types to provisioning operations submitted through Oracle Identity Manager.

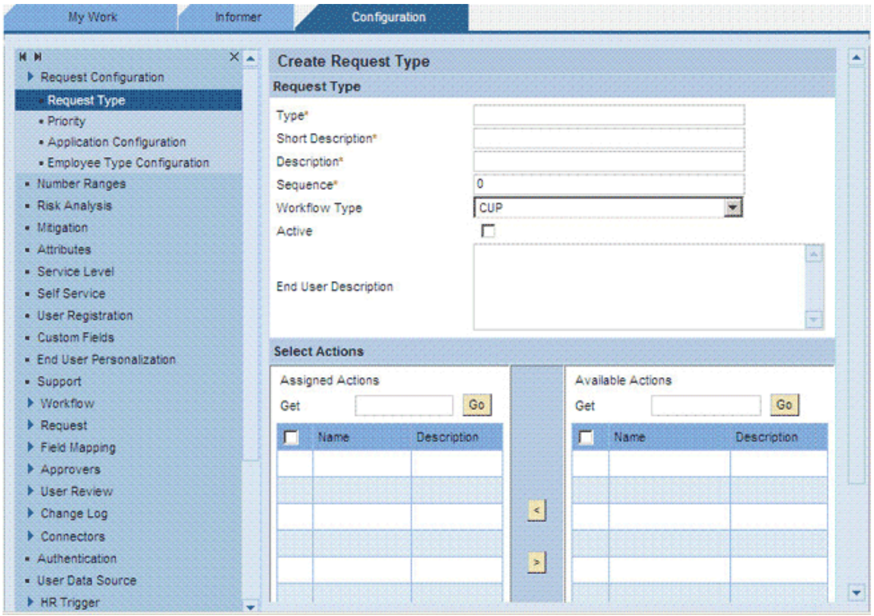
You can create request types in SAP GRC Compliant User Provisioning. Compliant User Provisioning also allows you to set default values for some user attributes. You can define these user defaults and then create user default mappings that specify conditions under which the user defaults must be applied.

To create a request type:

1. Log in to SAP GRC Access Control as an administrator.

2. On the Configuration tab, expand **Request Configuration**, click **Request Type**, and then click **Create**.

   The following screenshot shows this page:



Type*

Short Description*

Description*

Sequence* 0

Workflow Type CUP

Active □

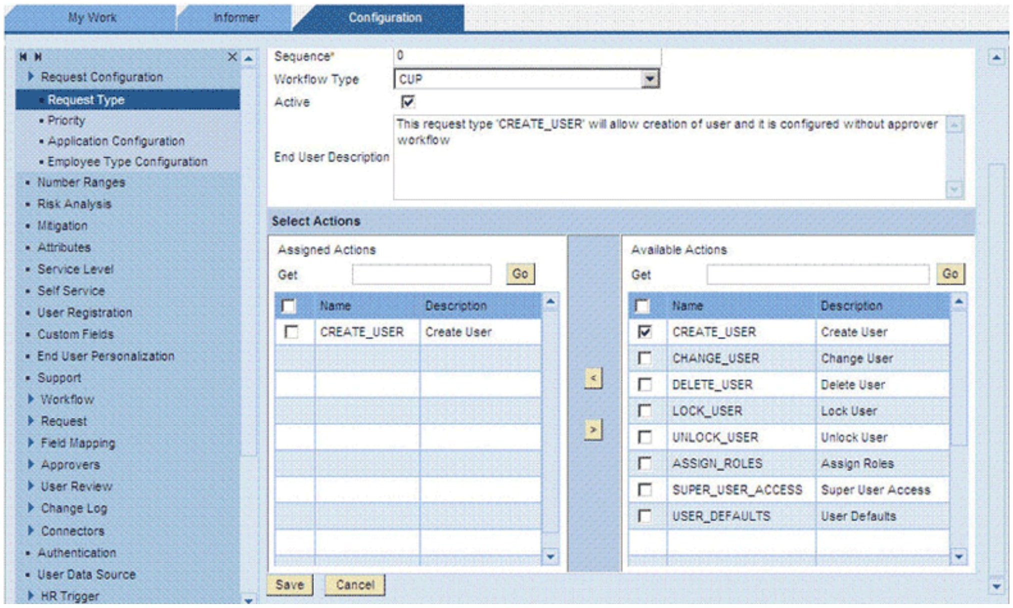
End User Description

3. Enter the following information about the request type:

   - Type: Enter a unique name for the request type. The name must be in uppercase.
   - Short Description: Enter a short description for the request type.
   - Description: Enter a description for the request type.
   - Sequence: Enter a numeric value for the sequence in which this request type must be displayed on the Request Access page. If you assign 0, then the request type does not appear on the Request Access page. However, if the request type is Active, then it appears in the Request Type list throughout SAP GRC Compliant User Provisioning.
   - Workflow Type: Select **CUP** as the workflow type.
   - Active: Select the check box to make the request type active.
   - End User Description: Enter a description for display to users.

4. The Select Actions region displays assigned actions and available actions. Assigned actions are actions that will be performed during provisioning. Available actions are actions that are available to be performed during provisioning. You can use the arrow icons to move actions from the Available Actions list to the Assigned Actions list.

   Select an action, and then click the left arrow to assign the action.



Sequence* 0

Workflow Type CUP

Active ☑

End User Description: This request type 'CREATE_USER' will allow creation of user and it is configured without approver workflow

Select Actions

Assigned Actions

Get

□	Name	Description
□	CREATE_USER	Create User

Available Actions

Get

□	Name	Description
☑	CREATE_USER	Create User
□	CHANGE_USER	Change User
□	DELETE_USER	Delete User
□	LOCK_USER	Lock User
□	UNLOCK_USER	Unlock User
□	ASSIGN_ROLES	Assign Roles
□	SUPER_USER_ACCESS	Super User Access
□	USER_DEFAULTS	User Defaults

5. Click **Save**.

2.3.7.3.2 Creating Workflows

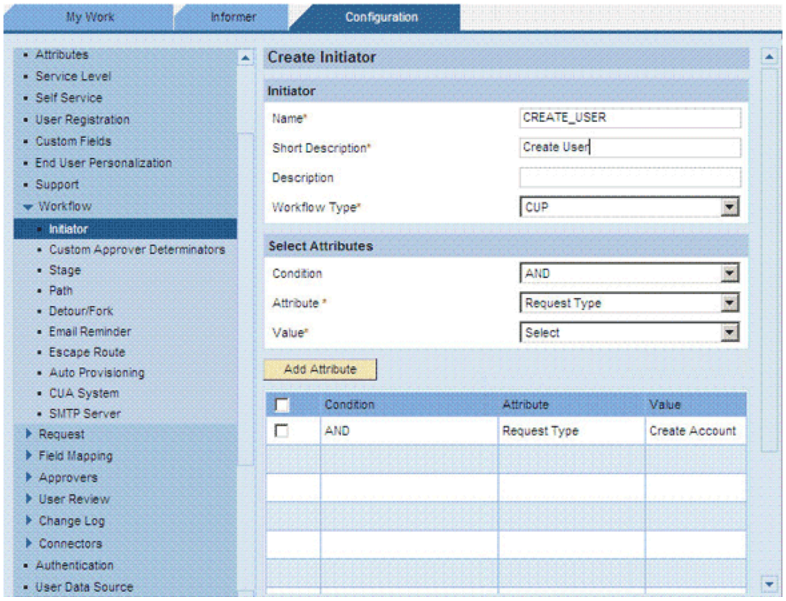
A workflow defined in SAP GRC Compliant User Provisioning acts upon a particular type of request. A workflow consists of an initiator, stage, and path. You can set up one workflow that contains all the request types. Alternatively, you can create a separate workflow for each request type.

An initiator is a combination of a request type and the workflow designed to handle that request type. Initiators and workflows function as matched pairs. A particular initiator can call only one workflow.

To create the initiator:

1. Log in to the SAP GRC Access Control as an administrative user.
2. On the Configuration tab, click **Workflow**, select **Initiator**, and then click **Create**.
3. Enter the following information about the initiator:
   - Name: Enter a name for the initiator. The name must be in uppercase. For example, enter `CHANGE_USER`.
   - Short Description: Enter a short description for the initiator.
   - Description: Enter a description for the initiator.
   - Workflow Type: Select **CUP** as the workflow type.
   - Select attribute information for the initiator:
   - Condition: Select **AND**, **NOT**, or **OR** as the condition. For this example, the OR condition is selected.
   - Attribute: Select **Request Typ**e as the attribute.
   - Value: Select a request type.
4. Click **Add Attribute**, and then repeat Step 3 for each request type that you create.
5. Click **Save**.

   The following screenshot shows this page:



Create Initiator

Initiator

Name*	CREATE_USER
Short Description*	Create User
Description	
Workflow Type*	CUP

Select Attributes

Condition	AND
Attribute *	Request Type
Value*	Select

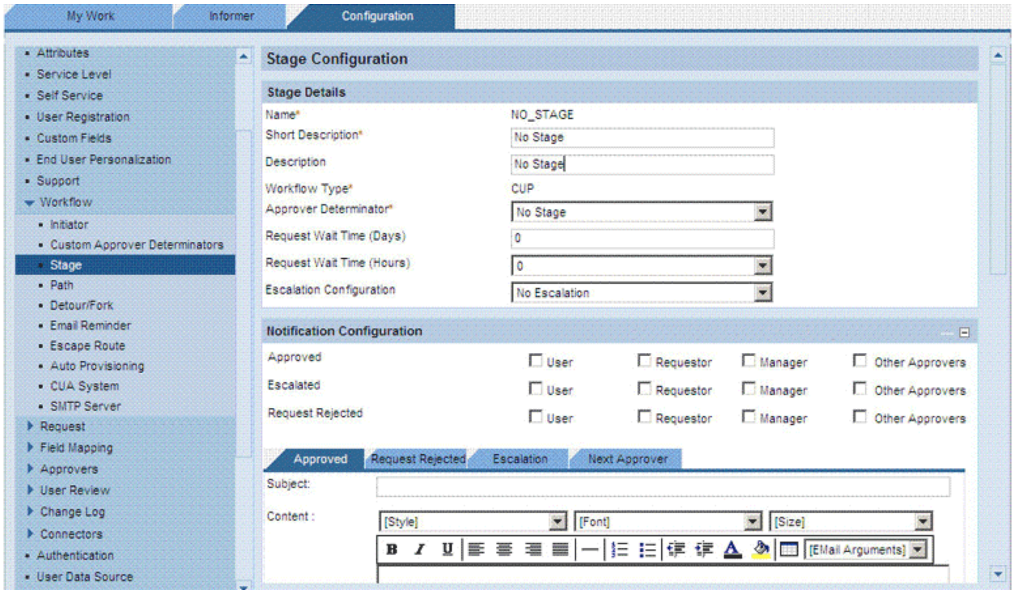
□	Condition	Attribute	Value
□	AND	Request Type	Create Account

A stage is a decision point in a workflow. At each stage in a workflow, an approver must approve or deny the request. The stage also specifies the action to be taken based on the decision of the approver. The request process proceeds beyond a stage only after the approver responds by approving or rejecting the request.

To create the stage:

1. Click **Workflow**, select **Stage**, and then click **Create**.
2. Enter the following information about the stage:
   - Name: Enter a name for the initiator. The name must be in uppercase, and it must not contain spaces. For example, enter `NO_STAGE`.
   - Short Description: Enter a short description for the initiator.
   - Description: Enter a description for the initiator.
   - Workflow Type: Select **CUP** as the workflow type.
   - Approver Determinator: Select a value according to your requirements.

     The following screenshot shows this page:



Stage Configuration

Stage Details

Name*	NO_STAGE
Short Description*	No Stage
Description	No Stage
Workflow Type*	CUP
Approver Determinator*	No Stage
Request Wait Time (Days)	0
Request Wait Time (Hours)	0
Escalation Configuration	No Escalation

Notification Configuration

Approved	□ User	□ Requestor	□ Manager	□ Other Approvers
Escalated	□ User	□ Requestor	□ Manager	□ Other Approvers
Request Rejected	□ User	□ Requestor	□ Manager	□ Other Approvers

Subject:

Content : [Style] [Font] [Size]

- Request Wait Time (Days): Enter the number of days for which Compliance User Provisioning must wait for an approver to respond to a request before escalating the request. In this example it is 0, because no escalation is configured.
- Request Wait Time (Hours): Enter the number of hours for which Compliance User Provisioning must wait for an approver to respond to a request before escalating the request. In this example it is 0, because no escalation is configured.
- Escalation Configuration: From the list, select **No Escalation**.
- Notification Configuration: Specify whether and to whom the system notifies about actions taken at this point in the stage.
- Additional Configuration: Define any additional functionality required at this stage.
- Additional Security Configuration: Specify whether or not approvers must reaffirm their actions by entering their password.

  The following actions can be configured to require password reaffirmation:

  – Approve

  – Reject

  – Create User (automatic creation of a user record)

3. Click **Save**.

A path defines the sequence of stages in a workflow. The stages in a workflow are related to other stages by the path.

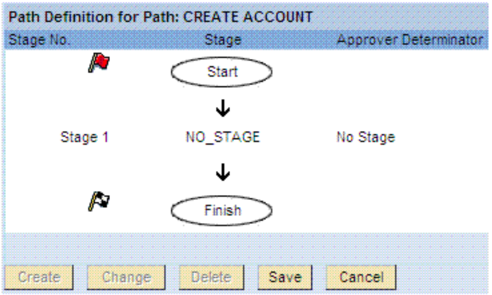
To create the path:

1. Click **Workflow**, select **Path**, and then click **Create**.
2. Enter the following information about the path:
   - Name: Enter a name for the path. The name must be in uppercase, and it must not contain spaces.
   - Short Description: Enter a short description for the path.

- Description: Enter a description for the path.
- Workflow Type: Select **CUP** as the workflow type.
- Number of Stages: Enter the number of stages that you want to include in the path.
- Initiator: From the list, select the initiator that you created earlier.
- Active: Select **Active** to make the path active.

3. Click Save to create the path.

   The following screenshot shows this page:



Path Definition for Path: CREATE ACCOUNT

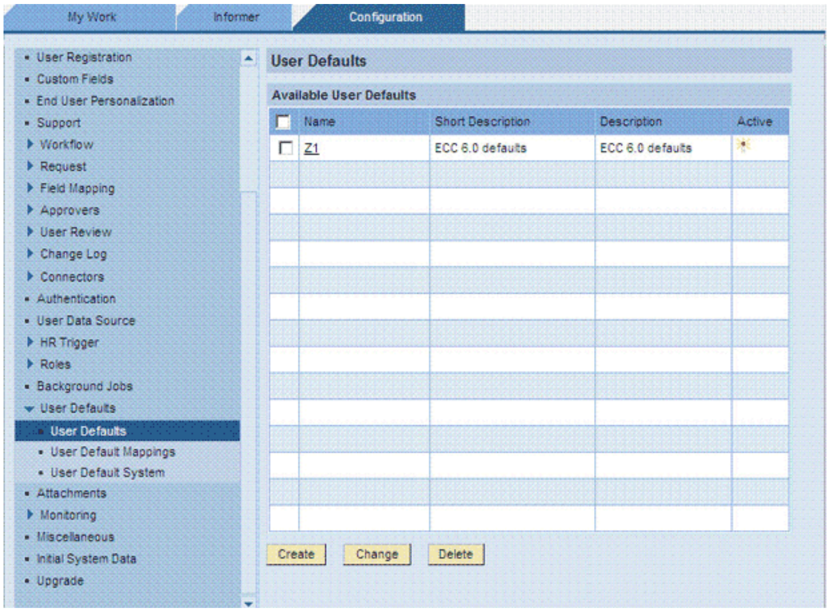
Stage No.	Stage	Approver Determinator
	Start	
Stage 1	NO_STAGE	No Stage
	Finish	

You can define a set of user defaults and also create user default mappings that define conditions under which the user defaults must be applied.

To define user defaults:

1. On the Configuration tab, expand **User Defaults** and then click **User Defaults**.

   The following screenshot shows this page:



User Defaults

Available User Defaults

□	Name	Short Description	Description	Active
□	Z1	ECC 6.0 defaults	ECC 6.0 defaults	✓

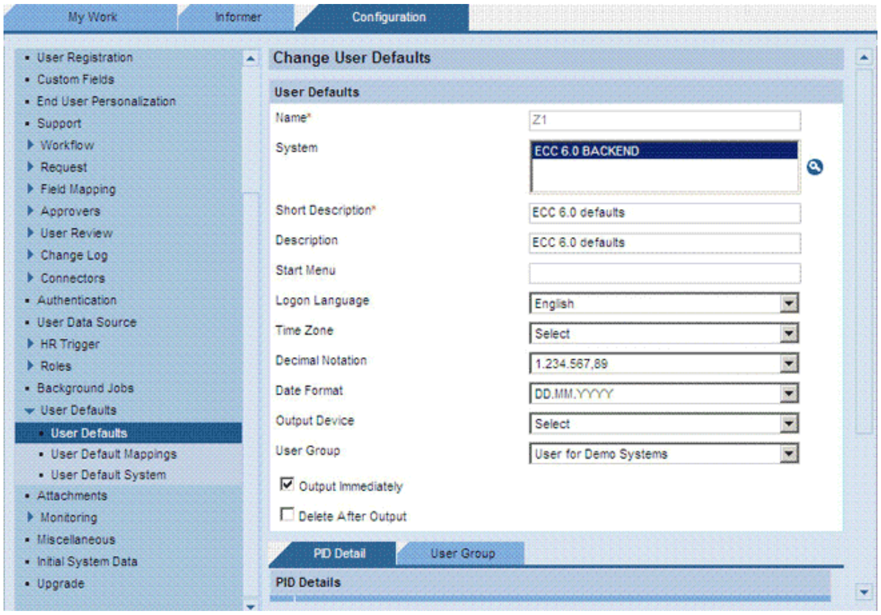
2. Enter values in the following fields:

   - Name: Enter a name for this set of user defaults.
   - System: Select the application with which the SAP User Management Engine data source is linked.
   - Short Description: Enter a short description for this set of user defaults.

- Description: Enter a description for this set of user defaults.

3. Specify default values for the Logon Language, Time Zone, Decimal Notation, Date Format, Output Device, and User Group attributes.

   The following screenshot shows this page:



Change User Defaults

User Defaults

Name*	Z1
System	ECC 6.0 BACKEND
Short Description*	ECC 6.0 defaults
Description	ECC 6.0 defaults
Start Menu	
Logon Language	English
Time Zone	Select
Decimal Notation	1.234.567,89
Date Format	DD.MM.YYYY
Output Device	Select
User Group	User for Demo Systems

☑ Output Immediately

☐ Delete After Output

PID Details

4. Click **Save**.

To define a user default mapping:

1. On the Configuration tab, expand **User Defaults** and then click **User Default Mappings**.
2. Enter values in the following fields:
   - Name: Enter a name for this set of user defaults.
   - Short Description: Enter a short description for this set of user defaults.
   - Description: Enter a description for this set of user defaults.
   - User Defaults: Select the default that you create.
3. In the Select Attributes region, use the Condition, Attribute, and Value lists to specify the attributes (conditions) under which the defaults must be applied.

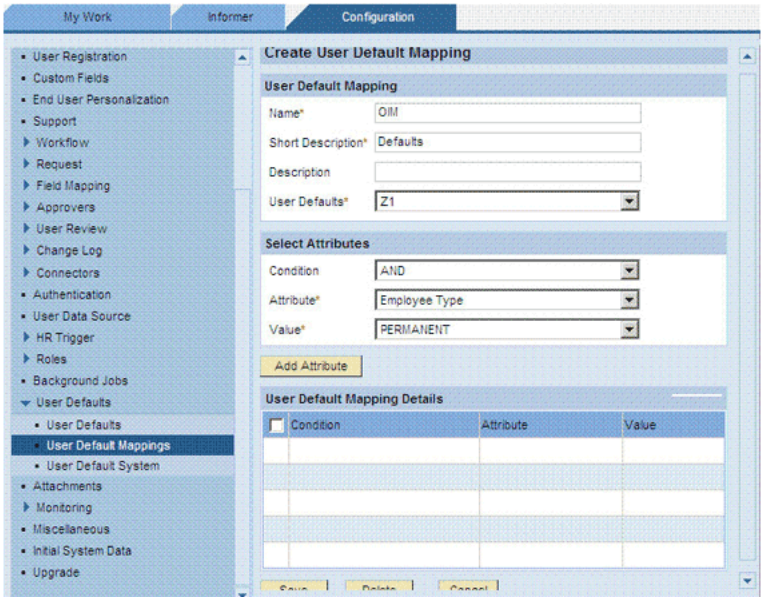
   For example, suppose you select the following attributes:

   Request Type: New

   Functional Area: Finance

   A request that has these two attributes is automatically assigned the user defaults.
4. Click **Save**.

   The following screenshot shows this page:



Create User Default Mapping

User Default Mapping

Name*: OIM

Short Description*: Defaults

Description:

User Defaults*: Z1

Select Attributes

Condition: AND

Attribute*: Employee Type

Value*: PERMANENT

User Default Mapping Details

2.3.7.4 Setting Values in the Lookup.SAP.CUP.Configuration Lookup Definition

Table 2–4 describes the entries in the Lookup.SAP.CUP.Configuration lookup definition.

> **Note:** You must not change any of the Code Key values of this lookup definition.

Table 2–4 Entries in the Lookup.SAP.CUP.Configuration Lookup Definition

Code Key	Description
Application	Enter the name of the system or application that is using the SAP User Management Engine data source. Sample value: `E60`
Assign Role	Enter the name of the request type that you create for Modify User provisioning operations. See Section 2.3.7.3.1, "Creating Request Types" for more information. Sample value: `MODIFY_USER`
Child Attribute Lookup	This entry holds the name of the lookup definition that stores child form attribute mappings for the Compliant User Provisioning feature. Value: `Lookup.SAP.CUP.ProvisionRoleAttrMap`
Constants Lookup	This entry holds the name of the lookup definition that stores values used by the connector in the Compliant User Provisioning feature. The connector development team can use this lookup definition to make minor configuration changes in the connector. Value: `Lookup.SAP.CUP.Constants`
Create User	Enter the name of the request type that you create for Create User provisioning operations. See Section 2.3.7.3.1, "Creating Request Types" for more information. Sample value: `CREATE_USER`

Table 2–4 (Cont.) Entries in the Lookup.SAP.CUP.Configuration Lookup Definition

Code Key	Description
Delete User	Enter the name of the request type that you create for Delete User provisioning operations. See Section 2.3.7.3.1, "Creating Request Types" for more information. Sample value: `DELETE_USER`
Ignore OPEN status	Use this entry to specify that new requests can be sent for a particular user, even if the last request for the user is in the Open status. If you set this entry to `yes`, then data from each new request replaces data stored from the preceding request, regardless of the status of the preceding request. If you set this entry to `no`, then new requests cannot be sent for a particular user for as long as the last request is in the Open status. Default value: `no` **Note:** If Ignore OPEN status is set to `no` and a new request is submitted for a user before an existing request for the user is closed, then a message is displayed on the Administrative and User Console. At the same time, the `Request ID xxx is in OPEN status` message is recorded in the log file.
Ignore User Created Check For Add Role	When an Add Role request is submitted through Oracle Identity Manager, the connector first checks if the specified user exists on the target system. If an approver is defined for the Create User request type and if the Add Role request is sent *immediately* after the Create User request is sent, then the process task for adding the role might be rejected. This is because the user is not created on the target system until SAP GRC Compliant User Provisioning clears the Create User request. If you want the connector to skip the check for the user on the target system during Add Role operations, then enter `yes` as the value of the Ignore User Created Check For Add Role entry. With this setting, the role is granted to the account (resource) in Oracle Identity Manager without checking if the user exists on the target system. Enter `no` as the value if you do not want to enable this feature. Default value: `yes`
IT Resource	This entry holds the name of the SAP GRC IT resource. Default value: `SAP GRC IT Resource`
Lock User	Enter the name of the request type that you create for Modify User provisioning operations. See Section 2.3.7.3.1, "Creating Request Types" for more information. Sample value: `LOCK_USER`
Modify User	Enter the name of the request type that you create for Modify User provisioning operations. See Section 2.3.7.3.1, "Creating Request Types" for more information. Sample value: `MODIFY_USER`

Table 2–4 (Cont.) Entries in the Lookup.SAP.CUP.Configuration Lookup Definition

Code Key	Description
Parent Attribute Lookup	This entry holds the name of the lookup definition that stores process form attribute mappings for the Compliant User Provisioning feature. Value: `Lookup.SAP.CUP.ProvisionAttrMap`
Priority	Enter the priority level at which SAP GRC Compliant User Provisioning must process requests sent from Oracle Identity Manager: ■ Low ■ Medium ■ High ■ Critical
Unlock User	Enter the name of the request type that you create for Modify User provisioning operations. See Section 2.3.7.3.1, "Creating Request Types" for more information. Sample value: `UNLOCK_USER`

2.3.8 Configuring SSL to Secure Communication Between the Target System and Oracle Identity Manager

To configure SSL between the target system and Oracle Identity Manager:

1. Generate the certificate on the target system.

   See the target system documentation for detailed instructions.

2. To import the certificate on Oracle Identity Manager:

   > **Note:** All application server releases supported by Oracle Identity Manager release 9.1.0.2 BP 04 and later are supported.
   >
   > In a clustered environment, you must perform this procedure on all the nodes of the cluster.

   a. Copy the target system certificate to the Oracle Identity Manager host computer.

   b. In a command window, change to the directory where you copy the certificate file and then enter a command similar to the following:

   ```
   keytool -import -alias ALIAS -file CER_FILE -keystore MY_CACERTS -storepass
   PASSWORD
   ```

   In this command:

   – *`ALIAS`* is the alias for the certificate (for example, the server name).

   – *`CER_FILE`* is the full path and name of the certificate (.cer) file.

   Table 2–5 shows the location of the certificate store for each of the supported application servers.

Table 2–5 Certificate Store Locations

Application Server	Certificate Store Location
Oracle WebLogic Server	■ If you are using Oracle jrockit_R27.3.1-jdk, then copy the certificate into the following directory: *JROCKIT_HOME*/jre/lib/security ■ If you are using the default Oracle WebLogic Server JDK, then copy the certificate into the following directory: *WEBLOGIC_HOME*/java/jre/lib/security/cacerts
IBM WebSphere Application Server	■ For a nonclustered configuration of any supported IBM WebSphere Application Server release, import the certificate into the following certificate store: *WEBSPHERE_HOME*/java/jre/lib/security/cacerts ■ For IBM WebSphere Application Server 6.1.*x*, in addition to the `cacerts` certificate store, you must import the certificate into the following certificate store: *WEBSPHERE_HOME*/AppServer/profiles/*SERVER_NAME*/config/cells/*CELL_NAME*/nodes/*NODE_NAME*/trust.p12 For example: C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv02\config\cells\wkslaurel3224Node02Cell\nodes\wkslaurel3224Node02\trust.p12 ■ For IBM WebSphere Application Server 5.1.*x*, in addition to the `cacerts` certificate store, you must import the certificate into the following certificate store: *WEBSPHERE_HOME*/etc/DummyServerTrustFile.jks
JBoss Application Server	*JAVA_HOME*/jre/lib/security/cacerts
Oracle Application Server	*ORACLE_HOME*/jdk/jre/lib/security/cacerts

c. To confirm whether or not the certificate has been imported successfully, enter a command similar to the following:

```
keytool -list -alias ALIAS -keystore MY_CACERTS -storepass PASSWORD
```

For example:

```
keytool -list -alias MyAlias -keystore
C:\mydir\java\jre\lib\security\cacerts -storepass changeit
```

d. For a nonclustered configuration of IBM WebSphere Application Server, download the jsse.jar file from the Sun Web site and copy this file into the *WEBSPHERE_HOME*/java/jre/lib/ext directory.

e. For a clustered configuration of IBM WebSphere Application Server, download the jnet.jar, jsse.jar, and jcert.jar files from the Sun Web site and copy these files into the *WEBSPHERE_HOME*/java/jre/lib/ext directory.

2.3.9 Configuring the IT Resource

The SAP UME IT Resource IT resource is automatically created when you run the Connector Installer. You must specify values for the parameters of the IT resource.

Note:

The ALL USERS group has INSERT, UPDATE, and DELETE permissions on the default IT resource. This is to ensure that end users can select the IT resource during request-based provisioning. If you create another IT resource, then you must assign INSERT, UPDATE, and DELETE permissions for the ALL USERS group on the IT resource.

You must use the Administrative and User Console to configure the IT resource. Values set for the connection pooling parameters will not take effect if you use the Design Console to configure the IT resource.

To specify values for the parameters of the IT resource:

1. Log in to the Administrative and User Console.
2. Expand **Resource Management.**
3. Click **Manage IT Resource**.
4. In the IT Resource Name field on the Manage IT Resource page, enter **SAP UME IT Resource** and then click **Search**.
5. Click the edit icon for the IT resource.
6. From the list at the top of the page, select **Details and Parameters**.
7. Specify values for the parameters of the IT resource. Table Table 2–6 describes each parameter.

Note: Entries in this table are sorted in alphabetical order of parameter names.

Table 2–6 Parameters of the IT Resource

Parameter	Description
Admin User ID	Enter the user ID of the target system user account that you create for connector operations See Section 2.1.2.1, "Creating a Target System User Account for Connector Operations" for more information.
Admin Password	Enter the password of the target system user account that you create for connector operations See Section 2.1.2.1, "Creating a Target System User Account for Connector Operations" for more information.

Table 2–6 (Cont.) Parameters of the IT Resource

Parameter	Description

UME URL	- If you perform the procedure described in Section 2.3.8, "Configuring SSL to Secure Communication Between the Target System and Oracle Identity Manager," then enter the URL for the SPML service in the following format:
	`https://`*`HOSTNAME`*`:`*`SSL_PORT`*`/spml/provisioning`
	- If you do not configure SSL between the target system and Oracle Identity Manager, then enter the URL for the SPML service in the following format:
	`http://`*`HOSTNAME`*`:`*`PORT`*`/spml/provisioning`
	Sample value: `http://myhost:50000/spml/provisioning`

Configuration Lookup	This parameter holds the name of the lookup definition containing configuration information. Value: `Lookup.SAP.UME.Configuration`
Dummy Password	Enter the dummy password that you want the connector to use during a Create User provisioning operation. The connector first sets the password as this value and then changes it to the password specified on the process form.

8. To save the values, click **Update**.

3

Using the Connector

This chapter is divided into the following sections:

> **Note:** These sections provide both conceptual and procedural information about configuring the connector. It is recommended that you read the conceptual information before you perform the procedures.

3.1 Performing Full Reconciliation

Full reconciliation involves reconciling all existing user records from the target system into Oracle Identity Manager. After you deploy the connector, you must first perform full reconciliation.

To perform a full reconciliation run, remove (delete) any value currently assigned to the Custom Recon Query attribute of the SAP UME User Recon scheduled task. See Section 3.6, "Configuring Scheduled Tasks" for information about this scheduled task.

3.2 Scheduled Task for Lookup Field Synchronization

The SAP UME Lookup Recon scheduled task is used for lookup field synchronization. Table 3–1 describes the attributes of this scheduled task. The procedure to configure scheduled tasks is described later in the guide.

Table 3–1 Attributes of the SAP UME Lookup Recon Scheduled Task

Attribute	Description
IT Resource	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. Default value: `SAP UME IT Resource`
Lookup Name	This attribute holds the name of the lookup definition that maps each lookup definition with the data source from which values must be fetched. Default value: `Lookup.SAP.UME.LookupMappings`
Schedule Task Name	This attribute holds the name of the scheduled task. Value: `SAP UME Lookup Recon`

3.3 General Considerations to Be Addressed While Using the Connector

Keep in mind the following points when you start using the connector:

- Multiple requests are generated from Oracle Identity Manager in response to some provisioning operations. For example, if you assign multiple roles to a user in a particular provisioning operation, then one request is created and sent to Compliant User Provisioning for each role.
- For a particular account, Oracle Identity Manager keeps track of the latest request only. This means, for example, if more than one attribute of an account has been modified in separate provisioning operations, then Oracle Identity Manager keeps track of data related to the last operation only.
- A Modify User operation can involve changes to multiple process form fields or child form fields. For each field that is modified, one request is created and sent to SAP GRC Compliant User Provisioning. Only information about the last request sent to Compliant User Provisioning is stored in Oracle Identity Manager.
- Only parent or child form requests can be submitted in a single operation. You cannot submit both parent and child form requests at the same time.

3.4 Guidelines on Performing Reconciliation

Apply the following guideline while configuring reconciliation:

- On a Microsoft Windows platform, if you encounter the org.quartz.SchedulerException exception during a reconciliation run, then download and install the Microsoft Visual C++ 2005 SP1 Redistributable Package from the Microsoft Web site.

3.5 Configuring Reconciliation

As mentioned earlier in this guide, reconciliation involves duplicating in Oracle Identity Manager the creation of and modifications to user accounts on the target system. This section discusses the following topics related to configuring reconciliation:

- Section 3.5.1, "Full Reconciliation"
- Section 3.5.2, "Limited Reconciliation"
- Section 3.5.3, "Reconciliation Scheduled Tasks"

3.5.1 Full Reconciliation

In full reconciliation, all existing target system records are fetched into Oracle Identity Manager for reconciliation. See Section 3.1, "Performing Full Reconciliation" for instructions.

3.5.2 Limited Reconciliation

In full reconciliation, all target system records are fetched into Oracle Identity Manager. You can also configure limited reconciliation to specify the subset of target system records that must be fetched into Oracle Identity Manager.

You configure limited reconciliation by specifying a query condition as the value of the Custom Query attribute of the SAP UME User Recon scheduled task.

You must use the following format to specify a value for the Custom Query attribute:

```
RESOURCE_OBJECT_FIELD_NAME equals VALUE
```

For example, suppose you specify the following as the value of the Custom Query attribute:

```
Last Name equals Doe
```

With this query condition, only records of users whose last name is `Doe` are brought for reconciliation.

> **Note:** The SPML API supports only one level of conditions, using either the AND or OR operator. Because the data source condition is already used in the connector code, only one additional condition can be specified in the custom reconciliation query.

To configure limited reconciliation:

1. Ensure that the attribute that you want to use in the query exists in the Lookup.SAP.UME.ReconAttrMap lookup definition.

   See Also: Table 1–4, " Entries in the Lookup.SAP.UME.ReconAttrMap Lookup Definition"

2. Create the query condition. Apply the following guidelines to create the query condition:

   - Use only the following operations in the query condition:

     > **Note:** If any other special character is included, then it is treated as part of the attribute value that you specify.

     – equals

     – startsWith

     – endsWith

     – like

   - Add a space before and after the operators used in the query condition. For example:

```
First Name startsWith John
```

This is to help the system distinguish between operators used in the query and the same characters included as part of attribute values specified in the query condition.

- Ensure that attribute names that you use in the query condition are in the same case (uppercase and lowercase) as the case of values in the Lookup.SAP.UME.ReconAttrMap lookup definition. For example, the following query condition would fail:

  ```
  fiRst Name startsWith John
  ```

3. While configuring the SAP UME User Recon scheduled task, specify the query condition as the value of the Custom Query attribute. The procedure is described later in this chapter.

3.5.3 Reconciliation Scheduled Tasks

You must specify values for the attributes of the following scheduled tasks:

> **Note:** Attribute values are predefined in the connector XML file that you import. Specify values only for the attributes that you want to change.

- Section 3.5.3.1, "SAP UME User Recon"
- Section 3.5.3.2, "SAP UME Delete Recon"
- Section 3.5.3.3, "SAP CUP Status Update Recon"
- Section 3.5.3.4, "SAP CUP Delete Recon"

3.5.3.1 SAP UME User Recon

You use the SAP UME User Recon scheduled task to reconcile user data from the target system. Table 3–2 describes the attributes of this scheduled task.

Table 3–2 Attributes of the SAP UME User Recon Scheduled Task

Attribute	Description
Attribute Mapping Lookup	This attribute holds the name of the lookup definition that stores attribute mappings for reconciliation. Value: `Lookup.SAP.UME.ReconAttrMap`
Child Attribute Mapping Lookup	This attribute holds the name of the lookup definition that stores child attribute mappings for reconciliation. Value: `Lookup.SAP.UME.ReconChildAttrMap`
Custom Query	Enter the query that you want the connector to apply during reconciliation. See Section 3.5.2, "Limited Reconciliation" for more information.
IT Resource	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. Default value: `SAP UME IT Resource`
Resource Object	This attribute holds the name of the resource object. Default value: `SAP UME Resource Object`

Table 3–2 (Cont.) Attributes of the SAP UME User Recon Scheduled Task

Attribute	Description
SAP System Time Zone	Enter the abbreviation for the time zone of the target system host computer. The value that you enter must be one of the time zones supported by the java.util.TimeZone class. **Note:** The connector does not validate the value that you enter. In addition, no error is thrown during reconciliation if the value entered is not a valid time zone. Sample value: `PST`
Schedule Task Name	This attribute holds the name of the scheduled task. Value: `SAP UME User Recon`
Full Recon Filter	This attribute holds the name of the lookup definition that stores characters supported by SAP User Management Engine. Value: `Lookup.SAP.UME.FullReconFilter`

3.5.3.2 SAP UME Delete Recon

You use the SAP UME Delete Recon scheduled task to reconcile deleted users from the target system. Table 3–3 describes the attributes of this scheduled task.

Table 3–3 Attributes of the SAP UME Delete Recon Scheduled Task

Attribute	Description
Disable User	Enter `yes` if you want the connector to disable accounts (in Oracle Identity Manager) corresponding to accounts deleted on the target system. Enter `no` if you want the connector to revoke accounts in Oracle Identity Manager. Default value: `no`
IT Resource	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. Default value: `SAP UME IT Resource`
Resource Object	This attribute holds the name of the resource object. Default value: `SAP UME Resource Object`
Schedule Task Name	This attribute holds the name of the scheduled task. Default value: `SAP UME Delete Recon`

3.5.3.3 SAP CUP Status Update Recon

You use the SAP CUP Status Update Recon scheduled task to fetch the status of provisioning requests sent to SAP GRC Compliant User Provisioning. For a particular user, only the status of the latest request is brought to Oracle Identity Manager. This request is the one currently stored on the process form. Table 3–4 describes the attributes of this scheduled task.

Table 3–4 Attributes of the SAP CUP Status Update Recon Scheduled Task

Attribute	Description
Constants Lookup	This attribute holds the name of the lookup definition that holds constants used by the connector during reconciliation and provisioning. Default value: `Lookup.SAP.CUP.Constants`
IT Resource	Enter the name of the IT resource for the SAP GRC installation from which you want to fetch request status data. Default value: `SAP GRC IT Resource`
Resource Object	This attribute holds the name of the resource object. Default value: `SAP UME Resource Object`
Schedule Task Name	This attribute holds the name of the scheduled task. Default value: `SAP CUP Status Update Recon`

3.5.3.4 SAP CUP Delete Recon

You use the SAP CUP Delete Recon scheduled task to revoke accounts (resources) of users in Oracle Identity Manager for whom the Create User provisioning requests are rejected by SAP GRC Compliant User Provisioning.

When you perform a Create User provisioning operation, the account is allocated to the OIM User even before SAP GRC Compliant User Provisioning clears the provisioning request and creates an account on the target system. For a particular user, if account creation on the target system fails, then the account provisioned in Oracle Identity Manager is an invalid account. You use the SAP CUP Delete Recon scheduled task to identify and delete such accounts.

Table 3–5 Attributes of the SAP CUP Delete Recon Scheduled Task

Attribute	Description
Configuration Lookup	This attribute holds the name of the lookup definition that stores configuration values used by the connector during reconciliation and provisioning. You can set values for some of the entries in this lookup definition. Default value: `Lookup.SAP.UME.Configuration`
Constants Lookup	This attribute holds the name of the lookup definition that holds constant values used by the connector during reconciliation and provisioning. Default value: `Lookup.SAP.CUP.Constants`
IT Resource	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. Default value: `SAP UME IT Resource`
Resource Object	This attribute holds the name of the resource object. Default value: `SAP UME Resource Object`
Schedule Task Name	This attribute holds the name of the scheduled task. Default value: `SAP CUP Delete Recon`

3.6 Configuring Scheduled Tasks

This section describes the procedure to configure scheduled tasks. You can apply this procedure to configure the scheduled tasks for lookup field synchronization and reconciliation.

Table 3–6 lists the scheduled tasks that you must configure.

Table 3–6 Scheduled Tasks for Lookup Field Synchronization and Reconciliation

Scheduled Task	Description
SAP UME Lookup Recon	This scheduled task is used for lookup field synchronization. Section 3.2, "Scheduled Task for Lookup Field Synchronization" describes this scheduled task.
SAP UME User Recon	This scheduled task is used for user record reconciliation. Section 3.5.3.1, "SAP UME User Recon" describes this scheduled task.
SAP UME Delete Recon	This scheduled task is used for reconciliation of deleted user records. Section 3.5.3.2, "SAP UME Delete Recon" describes this scheduled task.
SAP CUP Status Update Recon	This scheduled task is used to fetch the status of provisioning requests sent to SAP GRC Compliant User Provisioning. Section 3.5.3.3, "SAP CUP Status Update Recon" describes this scheduled task. **Note:** This scheduled task is created only if you configure the Compliant User Provisioning feature.
SAP CUP Delete Recon	This scheduled task is used to revoke accounts (resources) of users in Oracle Identity Manager for whom the Create User provisioning requests are rejected by SAP GRC Compliant User Provisioning. Section 3.5.3.4, "SAP CUP Delete Recon" describes this scheduled task. **Note:** This scheduled task is created only if you configure the Compliant User Provisioning feature.

To configure a scheduled task:

1. Log in to the Administrative and User Console.
2. Expand **Resource Management**.
3. Click **Manage Scheduled Task**.
4. On the Scheduled Task Management page, enter the name of the scheduled task as the search criteria and then click **Search**.
5. In the search results table, click the edit icon in the Edit column for the scheduled task.
6. On the Edit Scheduled Task Details page, you can modify the following details of the scheduled task by clicking **Edit**:
   - **Status:** Specify whether or not you want to leave the task in the enabled state. In the enabled state, the task is ready for use.
   - **Max Retries:** Enter an integer value in this field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the ERROR status to the task. The default value is 1.
   - **Next Start:** Use the date editor to specify the date when you want the task to run. After you select a date value in the date editor, you can modify the time value that is automatically displayed in the Next Start field.
   - **Frequency:** Specify the frequency at which you want the task to run.
7. After modifying the values for the scheduled task details listed in the previous step, click **Continue**.
8. Specify values for the attributes of the scheduled task. To do so, select each attribute from the Attribute list, specify a value in the field provided, and then click **Update**.

> **Note:** Attribute values are predefined in the connector XML file that you import. Specify values only for the attributes that you want to change.

The attributes of the scheduled task that you select for modification are displayed on this page.

9. Click **Save Changes** to commit all the changes to the database.

> **Note:** If you want to stop a scheduled task while it is running, then use the Stop Execution feature of the Design Console. See "The Task Scheduler Form" in *Oracle Identity Manager Design Console Guide* for information about this feature.

3.7 Guidelines on Performing Provisioning

Apply the following guidelines while performing provisioning operations:

- Through provisioning, if you want to create and disable an account at the same time, then you can set the value of the Valid Through attribute to a date in the past. For example, while creating an account on 31-Jul, you can set the Valid Through date to 30-Jul. With this value, the resource provisioned to the OIM User is in the Disabled state immediately after the account is created.

  However, on the target system, if you set the Valid Through attribute to a date in the past while creating an account, then the target system automatically sets Valid Through to the current date. The outcome of this Create User provisioning operation is as follows:

  – The value of the Valid Through attribute on Oracle Identity Manager and the target system do not match.

  – On the target system, the user can log in all through the current day. The user cannot log in from the next day onward.

  You can lock the user on the target system so that the user is not able to log in the day the account is created.

- When you try to provision a multivalued attribute, such as a role or group, if the attribute has already been set for the user on the target system, then the status of the process task is set to Completed in Oracle Identity Manager. If required, you can configure the task so that it shows the status Rejected in this situation. See *Oracle Identity Manager Design Console Guide* for information about configuring process tasks.

- When you perform the Lock User or Unlock User provisioning operation, remember that the connector makes the required change on the target system without checking whether the account is currently in the Locked or Unlocked state. This is because the target system does not provide a method to check the current state of the account.

- The target system does not accept non-English letters in the E-mail Address field. Therefore, during provisioning operations, you must enter only English language letters in the E-mail Address field on the process form.

- During a Create User operation performed when the Compliant User Provisioning is configured, first submit process form data. Submit child form data after the user is created on the target system. This is because when Compliant User Provisioning is enabled, the connector supports modification of either process form fields or child form fields in a single Modify User operation.

- The following fields on the process form are mandatory attributes on SAP GRC Compliant User Provisioning:

  > **Note:** You must enter values for these fields even though some of them are not marked as mandatory fields on the Administrative and User Console.

  – CUP Requestor ID

  – CUP Requestor First Name

  – CUP Requestor Last Name

  – CUP Requestor Email

  – GRC IT Resource

  – User ID

  – First Name

  – Last Name

  – E Mail

  The Valid From and Valid Through attributes are not mandatory attributes.

- As mentioned earlier in this guide, SAP GRC Compliant User Provisioning does not process passwords. Therefore, any value entered in the Password field is ignored during Create User provisioning operations. After a Create User operation is performed, the user for whom the account is created on the target system must apply one of the following approaches to set the password:

  – To use the Oracle Identity Manager password as the target system password, change the password through Oracle Identity Manager.

  – Directly log in to the target system, and change the password.

- You perform an Enable User operation by setting the Valid From field to a future date. Similarly, you perform a Disable User operation by setting the Valid Through field to the current date. Both operations are treated as Modify User operations.

- When you delete a user (account) on the Administrative and User Console (process form), a Delete User request is created.

- When you select the Lock User check box on the process from, a Lock User request is created.

- When you deselect the Lock User check box on the process from, an Unlock User request is created.

- The Enable User and Disable User operations are implemented through the Valid From and Valid Through fields on the process form.

- In a Modify User operation, you can specify values for attributes that are mapped with SAP GRC Compliant User Provisioning and attributes that are directly updated on the target system. A request is created SAP GRC Compliant User Provisioning only for attributes whose mappings are present in these lookup definitions. If you specify values for attributes that are not present in these lookup definitions, then the connector sends them to directly the target system.

- If an ABAP data source is configured in SAP User Management Engine, then ABAP roles are shown as groups in SAP User Management Engine. The group child form in Oracle Identity Manager shows these role details.

4

Extending the Functionality of the Connector

This chapter discusses the following optional procedures:

- Section 4.1, "Configuring Validation of Data During Reconciliation and Provisioning"
- Section 4.2, "Configuring Transformation of Data During User Reconciliation"
- Section 4.3, "Modifying Field Lengths on the Process Form"
- Section 4.4, "Configuring the Connector for Multiple Installations of the Target System"

4.1 Configuring Validation of Data During Reconciliation and Provisioning

You can configure validation of reconciled and provisioned single-valued data according to your requirements. For example, you can validate data fetched from the First Name attribute to ensure that it does not contain the number sign (#). In addition, you can validate data entered in the First Name field on the process form so that the number sign (#) is not sent to the target system during provisioning operations.

For data that fails the validation check, the following message is displayed or recorded in the log file:

```
Value returned for field FIELD_NAME is false.
```

> **Note:** This feature cannot be applied to the Locked/Unlocked status attribute of the target system.

To configure validation of data:

1. Write code that implements the required validation logic in a Java class.

   This validation class must implement the oracle.iam.connectors.common.validate.Validator interface and the validate method.

   > **See Also:** The Javadocs shipped with the connector for more information about this interface

   The following sample validation class checks if the value in the First Name attribute contains the number sign (#):

   ```
   public boolean validate(HashMap hmUserDetails,
   ```

```
        HashMap hmEntitlementDetails, String field) {
      /*
    * You must write code to validate attributes. Parent
    * data values can be fetched by using hmUserDetails.get(field)
    * For child data values, loop through the
    * ArrayList/Vector fetched by hmEntitlementDetails.get("Child Table")
    * Depending on the outcome of the validation operation,
    * the code must return true or false.
    */
    /*
    * In this sample code, the value "false" is returned if the field
    * contains the number sign (#). Otherwise, the value "true" is
    * returned.
    */
      boolean valid=true;
      String sFirstName=(String) hmUserDetails.get(field);
      for(int i=0;i<sFirstName.length();i++){
        if (sFirstName.charAt(i) == '#'){
              valid=false;
              break;
        }
      }
      return valid;
}
```

2. Create a JAR file to hold the Java class.
3. Copy the JAR file into the JavaTasks or ScheduleTask directory.
4. If you created the Java class for validating a process form field for reconciliation, then:
   a. Log in to the Design Console.
   b. Search for and open the **Lookup.SAP.UME.ReconValidation** lookup definition.
   c. In the Code Key, enter the resource object field name. In the Decode, enter the class name.
   d. Save the changes to the lookup definition.
   e. Search for and open the **Lookup.SAP.UME.Configuration** lookup definition.
   f. Set the value of the **Use Validation For Recon** entry to `yes`.
   g. Save the changes to the lookup definition.
5. If you created the Java class for validating a process form field for provisioning, then:
   a. Log in to the Design Console.
   b. Search for and open the **Lookup.SAP.UME.ProvValidation** lookup definition.
   c. In the **Code Key** column, enter the process form field name. In the **Decode** column, enter the class name.
   d. Save the changes to the lookup definition.
   e. Search for and open the **Lookup.SAP.UME.Configuration** lookup definition.
   f. Set the value of the **Use Validation For Prov** entry to `yes`.
   g. Save the changes to the lookup definition.

4.2 Configuring Transformation of Data During User Reconciliation

You can configure transformation of reconciled single-valued user data according to your requirements. For example, you can use First Name and Last Name values to create a value for the Full Name field in Oracle Identity Manager.

> **Note:** This feature cannot be applied to the Locked/Unlocked status attribute of the target system.

To configure transformation of single-valued user data fetched during reconciliation:

1. Write code that implements the required transformation logic in a Java class.

   This transformation class must implement the oracle.iam.connectors.common.transform.Transformation interface and the transform method.

   > **See Also:** The Javadocs shipped with the connector for more information about this interface

   The following sample transformation class creates a value for the Full Name attribute by using values fetched from the First Name and Last Name attributes of the target system:

```
package oracle.iam.connectors.common.transform;

import java.util.HashMap;

public class TransformAttribute implements Transformation {

      /*
      Description:Abstract method for transforming the attributes

      param hmUserDetails<String,Object>

      HashMap containing parent data details

      param hmEntitlementDetails <String,Object>

      HashMap containing child data details

      */
      public Object transform(HashMap hmUserDetails, HashMap
hmEntitlementDetails,String sField) {
      /*
       * You must write code to transform the attributes.
       Parent data attribute values can be fetched by
       using hmUserDetails.get("Field Name").
       *To fetch child data values, loop through the
       * ArrayList/Vector fetched by hmEntitlementDetails.get("Child
Table")
       * Return the transformed attribute.
       */
      String sFirstName= (String)hmUserDetails.get("First Name");
      String sLastName= (String)hmUserDetails.get("Last Name");
      String sFullName=sFirstName+"."+sLastName;
      return sFullName;
      }
}
```

2. Create a JAR file to hold the Java class.
3. Copy the JAR file into the JavaTasks or ScheduleTask directory.
4. If you created the Java class for transforming a process form field for reconciliation, then:
    a. Log in to the Design Console.
    b. Search for and open the **Lookup.SAP.UME.ReconTransformation** lookup definition.
    c. In the **Code Key** column, enter the resource object field name. In the **Decode** column, enter the class name.
    d. Save the changes to the lookup definition.
    e. Search for and open the **Lookup.SAP.UME.Configuration** lookup definition.
    f. Set the value of the **Use Transformation For Recon** entry to `yes`.
    g. Save the changes to the lookup definition.

4.3 Modifying Field Lengths on the Process Form

You might want to modify the lengths of fields (attributes) on the process form. For example, if you use the Japanese locale, then you might want to increase the lengths of process form fields to accommodate multibyte data from the target system.

> **Note:** On mySAP ERP 2005 (ECC 6.0 running on WAS 7.0), the default length of the password field is 40 characters. The default length of the password field on the process form is 8 characters. If you are using mySAP ERP 2005, then you must increase the length of the password field on the process form.

If you want to modify the length of a field on the process form, then:

1. Log in to the Design Console.
2. Expand **Development Tools**, and double-click **Form Designer**.
3. Search for and open the **UD_UME** process form.
4. Click **Create New Version**.
5. Enter a label for the new version, click the Save icon, and then close the dialog box.
6. From the **Current Version** list, select the version that you create.
7. Modify the length of the required field.
8. Click the Save icon.
9. Click **Make Version Active**.

4.4 Configuring the Connector for Multiple Installations of the Target System

You might want to configure the connector for multiple installations of the target system. The following example illustrates this requirement:

The London and New York offices of Example Multinational Inc. have their own installations of the target system. The company has recently installed Oracle Identity Manager, and they want to configure Oracle Identity Manager to link all the installations of the target system.

To meet the requirement posed by such a scenario, you can create copies of connector objects, such as the IT resource and resource object.

The decision to create a copy of a connector object might be based on a requirement. For example, an IT resource can hold connection information for one target system installation. Therefore, it is mandatory to create a copy of the IT resource for each target system installation.

With some other connector objects, you do not need to create copies at all. For example, a single attribute-mapping lookup definition can be used for all installations of the target system.

All connector objects are linked. For example, a scheduled task holds the name of the IT resource. Similarly, the IT resource holds the name of the configuration lookup definition, Lookup.SAP.UME.Configuration. If you create a copy of an object, then you must specify the name of the copy in associated connector objects. Table 4–1 lists associations between connector objects whose copies can be created and the other objects that reference these objects. When you create a copy of a connector object, use this information to change the associations of that object with other objects.

> **Note:** On a particular Oracle Identity Manager installation, if you create a copy of a connector object, then you must set a unique name for it.

Table 4–1 Connector Objects and Their Associations

Connector Object	Name	Referenced By	Comments on Creating a Copy
IT resource	SAP UME IT Resource	SAP UME User Recon (scheduled task) SAP UME Delete Recon (scheduled task) SAP UME Lookup Recon (scheduled task)	Create a copy of the IT resource. See Section 2.3.9, "Configuring the IT Resource" for more information.
Resource object	SAP UME Resource Object	SAP UME User Recon (scheduled task) SAP UME Delete Recon (scheduled task) SAP UME Lookup Recon (scheduled task)	It is optional to create a copy of the resource object. If you are reconciling the same set of attributes from all installations of the target system, then you need not create a copy of the resource object. In other words, create copies of the resource object only if there are differences in attributes between the various installations of the target system. See Section 3.5.3, "Reconciliation Scheduled Tasks" for more information.
Process definition	SAP UME Process Form	NA	Create copies of this process definition only if there are difference in attributes between the installations of the target system.

Table 4–1 (Cont.) Connector Objects and Their Associations

Connector Object	Name	Referenced By	Comments on Creating a Copy
Attribute Mapping Lookup Definition	Lookup.SAP.CUP.ProvAttrMap Lookup.SAP.CUP.ProvisionRoleAttrMap	NA	Create copies of these lookup definitions only if you want to map a different set of attributes for the various installations of the target system. See the following sections for more information: Section 1.6, "Connector Objects Used During Reconciliation" Section 1.7, "Connector Objects Used During Provisioning"
Process form	UD_UME	NA	It is optional to create a copy of a process form. If you are provisioning different sets of attributes, then you need to create a copy of this connector object.
Configuration lookup definition	Lookup.SAP.UME.Configuration	SAP UME IT Resource (IT resource)	Create copies of this lookup definition only if you want to use a different set of configuration values for the various installations of the target system. See Section 2.3.1, "Setting Values in the Lookup.SAP.UME.Configuration Lookup Definition" for more information.
Lookup mappings lookup definitions	Lookup.SAP.UME.LookupMappings	SAP UME Lookup Recon (scheduled task)	Create copies of these lookup definition only if you want to use a different set of lookup mappings for the various installations of the target system.

When you configure reconciliation:

To reconcile data from a particular target system installation, specify the name of the IT resource for that target system installation as the value of the scheduled task attribute that holds the IT resource name. For example, you enter the name of the IT resource as the value of the IT resource attribute of the SAP UME User Recon scheduled task.

When you perform provisioning operations:

When you use the Administrative and User Console to perform provisioning, you can specify the IT resource corresponding to the target system installation to which you want to provision the user.

4.4.1 Enabling the Dependent Lookup Fields Feature

When you perform a provisioning operation, lookup fields on the Administrative and User Console allow you to select values from lists. Some of these lookup fields are populated with values copied from the target system.

In earlier releases of the connector, if you had multiple installations of the target system, then entries in the lookup field were linked with the target system installation from which the entries were copied. This allowed you to select lookup field values that were specific to the target system installation on which the provisioning operation was to be performed.

For release 9.1.2 of the connector, the Dependent Lookup Fields feature is disabled by default. You can enable this feature after you deploy the Oracle Identity Manager release 9.1.0.2 bundle patch that addresses Bug 9181280.

Note: The bundle patch that addressed Bug 9181280 had not been released at the time of release of this connector.

To enable the Dependent Lookup Fields feature after you deploy the bundle patch that addresses Bug 9181280, you must make changes in the forms listed in Table 4–2. This table lists the forms, the lookup fields on the forms, and the lookup query that you must use for each lookup field. The procedure is described after the table.

Table 4–2 SQL Queries for Lookup Fields

Form	Lookup Field	Oracle Database Query for the Lookup Field	Microsoft SQL Server Query for the Lookup Field
UD_UMEGRP	Group Name	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UME.Groups' and instr(lkv_encoded,concat('$Form data.UD_UME_ITRESOURCE$','~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UME.Groups' and CHARINDEX('$Form data.UD_UME_ITRESOURCE$' + '~' ,lkv_encoded)>0
UD_UMERL	Role Name	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UME.Roles' and instr(lkv_encoded,concat('$Form data.UD_UME_ITRESOURCE$','~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UME.Roles' and CHARINDEX('$Form data.UD_UME_ITRESOURCE$' + '~' ,lkv_encoded)>0

To enable lookup fields on each form:

Note: You must enable lookup fields in the order given in Table 4–2.

1. On the Design Console, expand **Development Tools** and double-click **Form Designer**.
2. Search for and open the form. For example, open the UD_UME form.
3. Click **Create New Version**, enter a new version number, and then save the version.
4. From the **Current Version** list, select the version that you created.
5. Open the **Properties** tab, and expand **Components**.
6. Add properties for each lookup field on the form as follows:
   a. Select the **Lookup Code** property, and then click **Delete Property**.
   b. Select the first lookup field on the form, and then click **Add Property**. For example, select Profile System Name on the UD_UME form.
   c. In the Add Property dialog box:

      From the Property Name list, select **Lookup Column Name**.

      In the **Property Value** field, enter `lkv_encoded`.

      Click the Save icon, and then close the dialog box.
   d. Select the lookup field, and then click **Add Property**.
   e. In the Add Property dialog box:

From the Property Name list, select **Column Names**.

In the **Property Value** field, enter `lkv_encoded`.

Click the Save icon, and then close the dialog box.

f. Select the lookup field, and then click **Add Property**.

g. In the Add Property dialog box:

   From the Property Name list, select **Column Widths**.

   In the **Property Value** field, enter `234`.

h. Select the lookup field, and then click **Add Property**.

i. In the Add Property dialog box:

   From the Property Name list, select **Column Captions**.

   In the **Property Value** field, enter `lkv_decoded`.

   Click the Save icon, and then close the dialog box.

j. Select the lookup field, and then click **Add Property**.

k. In the Add Property dialog box:

   From the Property Name list, select **Lookup Query**.

   In the Property Value field, enter the query given in Table 4–2.

   Click the Save icon, and then close the dialog box.

7. Repeat Step 6 for each lookup field on the form.
8. Click the Save icon to save the changes to the form.
9. Click **Make Version Active**.

5 Known Issues and Limitations

This chapter is divided into the following sections:

- Section 5.1, "Known Issues"
- Section 5.2, "Connector Limitations Related to Features of the Target System"

5.1 Known Issues

The following is a known issue associated with this release of the connector:

- **Bug 7207232**

  Some Asian languages use multibyte character sets. If the character limit for fields on the target system is specified in bytes, then the number of Asian-language characters that you can enter in a particular field may be less than the number of English-language characters that you can enter in the same field. The following example illustrates this point:

  Suppose you can enter 50 characters of English in the User Last Name field of the target system. If you have configured the target system for the Japanese language, then you would not be able to enter more than 25 characters in the same field.

  See Section 4.3, "Modifying Field Lengths on the Process Form" for information about working around this issue.

5.2 Connector Limitations Related to Features of the Target System

The following are connector limitations related to features of the target system:

- The SPML UME API does not return records for which the Last Modified Date value is greater than a specified date. Therefore, the connector cannot support incremental reconciliation.
- Request-based provisioning is not supported. Because provisioning operations are routed through the Compliant User Provisioning module, the request-based provisioning feature of that module makes the feature in the connector redundant.
- Configurable batched reconciliation is not supported. The connector performs batched reconciliation implicitly when it first fetches user IDs whose records must be reconciled and then fetches the records.

Index